**Logo

Description automatically generated**

**­­**

**CSI-COP MOOC:**

**Az online adatvédelemhez való jog -**

**2. változat**

**Civil Kutatók Vizsgálják A Sütik És Appok GDPR Megfelelőségét**

**Tartalom**

**CSI-COP MOOC – informális oktatást nyújtó tanfolyam 2. oldal**

**A tanfolyam részletei 4. oldal**

**1. lépcső: Adatvédelem 5. oldal**

**2. lépcső: Adatok 10. oldal**

**3. lépcső: Online nyomkövetés 16. oldal**

**4. lépcső: Adatvédelemhez való jog 23. oldal**

**5. lépcső: Az adatvédelem eszközei 27. oldal**

**Az Ön visszajelzése a tanfolyamról 32. oldal**

**Ellenőrző kérdések 33. oldal**

**Hogyan lehet civil kutatóvá válni? 35. oldal**

**Kérdőív 36. oldal**

### **MOOC**

A CSI-COP ingyenes, informális oktatást nyújtó, rövid tanfolyama (massive open, online course - MOOC) elvégezhető online, vagy egy letölthető dokumentum formájában. A MOOC elvégzése 2,5-3 órát vesz igénybe.

A MOOC az Ön **adatairól és az online adatvédelemhez való jogáról szól**. Az interneten jelen lévő adatok gyűjtése digitális technológiák segítségével történik a weboldalakon és az alkalmazásokban (a mobil eszközök szoftvereiben). Ezek a technológiák magukban foglalják a sütiket: az asztali számítógépeken, laptopokon vagy okos eszközökön (táblagépeken, mobiltelefonokon) elhelyezett kis szöveges fájlokat, amelyekkel egy internetes oldal felkeresésekor találkozhat. A sütik között vannak digitális nyomkövetők, amelyek például eszköze pontos helyének nyomon követését végzik. Az alkalmazásbeállítások engedélyezhetik az Ön névjegyeinek, fényképezőjének, üzeneteinek, mikrofonjának és más adatainak elérését a mobil eszközein. Egy adott eszköz helye azonosíthatja az eszközt használó vagy birtokló személyt, így annak nyomon követése adatvédelmi vonzatokkal bír.

A [EU Horizont 2020](https://cordis.europa.eu/project/id/873169) programja által támogatott [CSI-COP](https://csi-cop.eu/) projekt fő célja a nagyközönség informális oktatása az online nyomkövető technológiákról és azok kiiktatásának módjáról. Ennek eredményeként a nagyközönség soraiból „civil kutatók” kerülhetnek ki. A civil kutató (citizen scientist - CS) a nagyközönség tagja, aki adatok gyűjtésével és elemzésével foglalkozik hivatásos kutatókkal folytatott együttműködés keretében. A CSI-COP célja, hogy civil kutatókat vonjon be, akik **a CSI-COP projekt csapatához csatlakozva** vizsgálják, hogy a nyomkövetés milyen mértékben tekinthető alapértelmezettnek az interneten. A 2018. évi általános adatvédelmi rendelet (General Data Protection Regulation - **GDPR**) ellenőrző listát kínál, amely alapján értékelhető a rendeletnek való megfelelés. A CSI-COP csapata hisz abban, hogy szükség van a civil tudományos megközelítésre az állampolgárok és a tudósok közötti együttműködés megteremtéséhez, valamint annak felderítéséhez, hogy adatainkat milyen mértékben követik online az általunk látogatott weboldalakon és az általunk használt alkalmazásokban.

Kinek szól ez a tanfolyam?

A tanfolyam minden olyan, 18. életévét betöltött személy, illetve tanári felügyelet mellett minden olyan diák számára megfelelő, akit érdekel, hogyan gyűjtik adatainkat az interneten és az általunk használt alkalmazásokon keresztül, és aki meg akarja tudni, hogyan védhetjük meg magánéletünket online.

Mire van szükség a tanfolyam sikeres elvégzéséhez?

Internet hozzáféréssel rendelkező okostelefon, táblagép, laptop vagy számítógép használatára van szükség. Ingyenes wi-fi hozzáférés is lehetséges, ha egyetemen, vagy helyi könyvtárban tartózkodik, de kérjük, vegye figyelembe, hogy az ingyenes, nyilvános wi-fi előnyei mellett azzal a veszéllyel jár, hogy hackerek hozzáférhetnek az Ön adataihoz. Kérjük, olvassa el a [Kaspersky](https://www.kaspersky.co.uk/resource-center/preemptive-safety/public-wifi-risks) tájékoztatását a nyilvános wi-fi veszélyeinek elkerüléséről: <https://bit.ly/3v6thff>

Amennyiben Twitter-t használ

Minden lépcső végén javaslatot teszünk egy rövid üzenetre, amelyet másoknak elküldve tudathatja velük, hogy részt vesz a CSI-COP informális oktatást nyújtó tanfolyamán. Használhatja a CSI-COP-ot jelölő címkét: [@cop\_csi](https://twitter.com/cop_csi?lang=en).

**Kérjük, tekintse meg a tanfolyam részleteit a 4. oldalon, majd próbálja ki az informális tanulás 1., 2., 3., 4. és 5. lépcsőjét az 5. oldaltól.**

Minden lépcsőnél röviden bemutatjuk a tananyagot és az új ismereteket, háttérinformációként pedig megadjuk az olvasnivalókhoz vezető linkeket és azok szerzőit is. További részletek találhatók az egyes lépcsők végén a További olvasnivalók részben.

A tanulás és megértés elmélyítése érdekében kérjük, hogy minden lépcsőben fordítson figyelmet a **fő kérdésre**. Ez arra biztatja, hogy fontolja meg az adott témát, mielőtt tanulna róla. Ezt, illetve az egyéb kérdéseket is megvitathatja a családjával és a barátaival, vagy beszélgethet másokkal a CSI-COP weboldal [fórum](https://csi-cop.eu/forum/)án. Ehhez először regisztrálnia kell az alábbi linken:

<https://csi-cop.eu/citizenscientistlogin/>

Minden lépés után lehetősége lesz ellenőrizni a tanultakat, amiben feladatok segítenek.

Az utolsó lépcső után az egész tanfolyam áttekintésére szolgáló részt talál. Emellett az 5. lépcső után információt nyújtunk arról, hogyan csatlakozhat a CSI-COP csapathoz, hogy civil kutatóként vizsgálja az online adatvédelmet, és **adatvédelmi bajnokká** válhasson.

Kellemes időtöltést!

**A TANFOLYAM RÉSZLETEI**

|  |  |
| --- | --- |
| **CSI-COP MOOC: informális oktatást nyújtó, önállóan végezhető tanfolyam** | *Az online adatvédelemhez való jog* |
| **A MOOC céljai** | A CSI-COP ingyenes online tanfolyama **öt lépcsőből** áll. Az egyes lépcsőfokokon végighaladva Ön megfelelő ismereteket szerez, hogy megalapozott döntéseket hozzon az online adatvédelemhez való jogaival kapcsolatban, és felvérteződik az interneten és az androidos eszközök (pl. Samsung mobil vagy táblagép) alkalmazásaiban működő nyomkövető technológiák ellenőrzéséhez és blokkolásához szükséges készségekkel. A tanfolyam öt lépcsőjének elvégzése után igényelheti a CSI-COP informális oktatásáról szóló bizonyítványt. Ezután a CSI-COP csapathoz csatlakozva informális tanulóból önkéntes civil kutatóvá válhat, hogy megvizsgálja, milyen mértékben követik nyomon adatait az interneten (ld. az 5. lépcsőt).  A CSI-COP projekt oldala az Európai Unió pályázati felületén:  [**https://cordis.europa.eu/project/id/873169**](https://cordis.europa.eu/project/id/873169) |
| **Mit tanulhat meg?** (*Elsajátítandó ismeretek*) | 1. Az emberi jogi egyezményekben biztosított adatvédelemmel kapcsolatos ismeretek 2. A weboldalakba és az androidos alkalmazásokba beágyazott online nyomkövető technológiák feltárásával kapcsolatos gyakorlati készségek (*know-how*) 3. Hogyan válhat civil kutatóvá, és hogyan csatlakozhat a CSI-COP csapathoz, hogy megvizsgálja a digitális nyomkövető technológiákkal folytatott online nyomkövetés mértékét |
| **A tanfolyam időtartama** | A tanfolyam a következő módokon végezhető el:   * Mind az öt lépcső egyszerre, beleértve az informális tanulást és a feladatokat: **2,5-3 óra alatt** * A saját tempójában |
| **Az informális oktatás részletei** | |
| **Cím** | *Adatai védelme* |
| **Célok és rövid leírás** | Ezt a workshopot úgy terveztük, hogy fél nap alatt, egyszerre teljesíthető legyen. A tananyag lépésein azonban időbeosztásának megfelelően több szakaszban is végighaladhat.  Az online workshopon Ön átfogó ismereteket szerez majd az adatvédelem különböző vonatkozásairól, illetve arról, hogyan használhatják fel harmadik felek az Ön személyes adatait a weboldalakon és az alkalmazások használatakor történő online interakciói során. Megtudhatja, hogyan lehet megalapozott döntéseket hozni személyes adataival kapcsolatban, és hogyan lehet ellenőrizni az Önről szóló adatok gyűjtésének átláthatóságát. |
| **Mit tanulhat meg?**  - (Új *ismeretek*) | **A tanfolyam végeredményeként Ön képessé válik arra, hogy:**   1. Leírja és megvitassa az adatvédelem különböző szempontjait. 2. Azonosítsa és értékelje a személyes adatok gyűjtésének módját az interneten való szörfölés és az okos eszközök alkalmazásainak használata során. 3. Megértse az adataink védelmét biztosító egyezményekből eredő adatvédelmi jogokat. |
| **A tanfolyam tartalma** | * Adatvédelem és annak különböző szempontjai * Mi a személyes adat? * Hogyan gyűjtik a személyes adatokat az internethasználatunk során? * Adatvédelemhez való jog (ENSZ, EU, GDPR) * Adataink online védelme. |

### 1. lépcső

|  |  |
| --- | --- |
| 1. lépcső címe | Az adatvédelem különböző szempontjai |
| Új ismeretek az 1. lépcsőben | 1. Az adatvédelem különböző szempontjainak leírása és megvitatása. |
| Téma | Adatvédelem és annak különböző szempontjai |
| Fő kérdés | *Az adatvédelem kiváltság, vagy emberi jog?*  Kérdezze meg a családját és a barátait, hogy mit gondolnak az **adatvédelem**ről. Posztolhatja meglátásait a CSI-COP honlap fórumán: <https://csi-cop.eu/forum/>. Mielőtt posztol a fórumon, egy log-in létrehozásával regisztrálnia kell a honlapon: <https://csi-cop.eu/citizenscientistlogin/> |
| Rövid összefoglaló | Jan Holvast (2009) “Discussion on privacy issues is as old as mankind”.  [Lásd a további olvasnivalók részt az 1. lépcső végén] |
|  |  |
| Tananyag | **Az ‘adatvédelem’ rövid története**  Jan Holvast (2009) szerint “Az adatvédelmi kérdésekkel kapcsolatos vita egyidős az emberiséggel. A **saját test és az otthon védelmével** kezdődött, majd rövidesen a **személyes adatok ellenőrzésének irányába** fejlődött.”  A picture containing text, screenshot, electronics, computer  Description automatically generated  1890-ban Warren és Brandeis ezt írta “Az elv, hogy az egyén élvezze személyének és tulajdonának teljes védelmét egyidős a szokásjoggal”, és “a korai időkben a jog csak az élet és tulajdon elleni fizikai támadással szemben nyújtott védelmet”. Hozzátették, hogy “jelenleg [1890-ben] az élethez való jog jelentése … a békénhagyás jogává változott”, és “a ‘tulajdon’ kifejezés magában foglalja a birtokolt javak minden formáját – mind az immateriálist, mind a kézzelfoghatót”.  2011-ben Nissenbaum arról adott tájékoztatást, hogy “A 2010-es év nagy év volt az online adatvédelem szempontjából. Adatvédelmi baklövésekkel, mint például a Google Buzz és a Facebook megbízhatalan adatvédelmi eljárásával kapcsolatos jelentések díszelegtek a vezető mediumok első oldalán. “**On What They Know**” című sorozatában a The Wall Street Journal ráirányította a figyelmet arra, hogy viselkedésalapú hirdetések céljából és más okokból erőszakosan követik az egyéneket.”  *Az adatvédelem etikája* tekintetébenMarijn Sax (2018) a következő kérdésekre összpontosít: ‘**Mi az adatvédelem értéke?**’ és ***‘*Milyen adatvédelmi normákra kell tekintettel legyen az egyén (önmagunkat is beleértve), a társadalom és az állam?**’  2022. április 10-én John Oliver brit humorista az HBO-n futó, Last Week Tonight című műsorában „felhívta a figyelmet az adatbrókerek által okozott károkra, akik felszedegetik és összeillesztik digitális adataink darabkáit, hogy megfosszanak minket a névtelenségtől, és harmadik feleknek adják el adatainkat” (Guardian, 2022. április 11.) Oliver beszámolt róla, hogy az adatbrókerek egy „multimilliárd dolláros iparág részei”, amely „összegyűjti az Önre vonatkozó személyes információkat, és ezeket továbbadja, illetve megosztja másokkal”. Mindennek „elsődleges eszközei a sütik, amelyek lehetővé teszik a weboldalak számára, hogy megjegyezzék Önt, és amelyek már harmadik felek sütijeit is magukban foglalják, amelyek azt is követik, hogy milyen egyéb helyeket keres még fel az interneten” (Guardian). A sütikre még visszatérünk a tanfolyam 3. lépcsőjben.  **Google Chrome**  Néhányan a Google Chrome kereső ***Incognito*** módját használják adataik védelme érdekében. De úgy tűnik, hogy a Google “titokban az internetes adatok kincsestárát hozza létre akkor is, ha a felhasználó “Incognito” módot használ keresési történetének titokban tartására.” (Nayak és Rosenblatt, 2021). Egy 2021 évi Bloomberg jelentés szerint “Fogyasztók keresetet nyújtottak be “közös akcióként”, azt állítva, hogy “még akkor is, ha kikapcsolják az adatgyűjtést, a Chrome vagy a honlapok által használt más Google eszközök hatalmas mennyiségű személyes adatot gyűjtenek” (Nayak és Rosenblatt, 2021). Erről az esetről továbbiak a Bloomberg új honlapján <https://bloom.bg/3gFt4vV> olvashatók.  **Facebook: 533 millió felhasználói adatsértés**  Talán hallotta a közelmúlt hírét, hogy bármennyire is igyekszünk adatainkat védeni, ha közösségi médiát használunk, akkor a platform tulajdonosának rendelkezésére állunk és szakértelmére szorulunk adataink védelme szempontjából. **Több mint 530 millió Facebook felhasználó személyes adatai váltak elérhetővé egy honlapon hackerek számára 2021 áprilisában** (Holroyd, 2021). Az 533 millió Facebook felhasználó, akinek személyes adatai eléhetővé váltak a következő országokból kerültek ki:   * több mint 35 millió Olaszországból * több mint 32 millió az USA-ból * közel 20 millió fiók Franciaországból * 11 millió felhasználó az Egyesület Királyságból és * 6 millió felhasználó Indiából.   Lomas (2021) leírja, hogy az adathalmaz, melyet a Facebook felhasználók megosztottak ezen a platformon a következőket tartalmazta:   * Facebook ID-k * teljes nevek * telefonszámok * tartózkodási helyek * születésnapok * önéletrajzok és * néhány email cím.   Több is olvasható erről a témáról a [TechCrunch](https://techcrunch.com/2021/04/06/answers-being-sought-from-facebook-over-latest-data-breach/?guce_referrer=aHR0cHM6Ly93d3cuZ29vZ2xlLmNvbS8&guce_referrer_sig=AQAAAMUOIlLG_dSDm7w74IG-14xWYBlW6py7Mv17hgb8XiPn2uZ7Dkrhgu4A0krDDh0ttvoqMkev6D_h7Man-RtR7mMGNmk5i1_oayagVtIi3W8g3McHb1cTXnWDGzLr9fUa3u1DIYa3yMFn1UCx2zMqgcF9J0G_2nP_mU6aSU41mLXG&guccounter=2)-on.  Ha Facebook felhasználó, és szeretné kideríteni, hogy a személyes adatai részét képezik-e ennek az adatsértésnek, ezt megteheti emailben, vagy Facebook ID-ját, illetve telefonszámát használva az alábbi honlapokon:   * [Have I been pwned?](https://haveibeenpwned.com/) itt: <https://haveibeenpwned.com/> * [Have I been Zucked?](https://haveibeenzucked.com/) itt: <https://haveibeenzucked.com/>   Követheti az erről szóló tweet-eket is itt [The Real Facebook Oversight Board](https://twitter.com/FBoversight) a “holding Facebook to account” címen: <https://twitter.com/FBoversight>  Talán Ön is hallott [Frances Haugen](https://twitter.com/FrancesHaugen?ref_src=twsrc%5Egoogle%7Ctwcamp%5Eserp%7Ctwgr%5Eauthor) adattudósról, a Facebook korábbi alkalmazottjáról. Haugen az USA Szenátusa előtt 2021. október 5-én, az Egyesült Királyság Parlamentjében 2021. október 25-én, az Európai Parlamentben pedig 2021. november 8-án tett tanúvallomást. Ezekben leleplezte a Facebook stratégiáját, amely a felhasználók érdekeinek rovására igyekszik profitra szert tenni. (További olvasnivalók Frances Haugen érdekvédelmi tevékenységéről, amelyet a “közösségi media elszámoltathatósága és átláthatósága” érdekében fejt ki: <https://www.franceshaugen.com/>).  Írország adatvédelmi bizottsága 17 millió eurós bírságot vetett ki a Meta Platforms Ireland Limited-re a 2018. június 7. és december 4. között történt sorozatos adatsértések miatt. (Forrás: <https://bit.ly/3MmUIKN> ).  Christopher Wylie, a Cambridge Analytica korábbi adattudósának és a 2019-es “MindF\*ck: Inside Cambridge Analytica’s Plot to Break the World” c. könyv szerzőjének kijelentése szerint “a Facebook túlságosan nagy, ellenőrizetlen hatalommal rendelkezik” (225. old.).  2021-ben az Egyesült Államok New York-i Déli Kerületi Bírósága polgári pert indított Google Digital Advertising Antitrust címen. Az Egyesült Államok bírósági dokumentumának 64. oldalán található 175. bekezdés kimondja:  „A Google azt a nyilvános képet mutatja, hogy törődik az adatvédelemmel, de a színfalak mögött a Google szorosan együttműködik a Big Tech vállalataival, hogy lobbizzon a kormánynál olyan intézkedések késleltetése vagy megsemmisítése érdekében, amelyek ténylegesen védenék a felhasználók magánéletét” (1. számú polgári keresetből: 21-md-03010-PKC dokumentum, amely a courtlistener.com webhelyről érhető el).  Carissa Veliz, a 2020-as “Privacy is Power” c. könyv szerzőjének figyelmeztetése szerint:   * + “Az internetet elsősorban az adatok gyűjtése, elemzése és kereskedelme … az adatgazdaság finanszírozza” (1. old.)   + “Ezen adatok nagy része személyes adat – az Ön adata” (1. old.)   + “ … az okostelefonok …. rögzítik az Ön útját, és hogy mennyi ideig maradt….” (2. old.)   + “ Az adatgazdaság, és a mindent átható megfigyelés, amelyből táplálkozik, meglepetésként ért bennünket” (2. old.)     A kép szövege:  **Az adatévdelem újragondolása: helyadatok?**  Hol vagyok most? + tevékenység/helyzet/SSID (Wi-fi név)  Hol nem vagyok (általában)?  Hová tartok?  Merre jártam?  Milyen útvonalon haladtam?  Milyen irányba nézek? / Milyen magasan vagyok?  Milyen személyekhez és dolgokhoz kapcsolódom?  Mire számíthat a következő lépcsőkben  A következő lépcsőben (2. lépcső) elkezdjük az *adatok* és a *személyes adatok* vizsgálatát.  A 3. lépcsőben megnézzük, hogy hogyan *követik adatainkat*.  A 4. lépcsőben megvizsgáljuk, hogy milyen *jogaink* vannak *adataink védelmére*.  A tanfolyam utolsó lépcsőjében, az 5. lépcsőben azokról az *online eszközökről* fogunk tanulni, amelyeket *adataink hatékonyabb védelmére* használhatunk.  Ellenőrizze a tanultakat!  Kérem, ellenőrizze az alábbi kérdéssel és két feladattal, hogy mit tanult az 1. lépcsőben! |
| Ellenőrizze tudását | Mi az *adatvédelem*? |
| Feladatok | **1.feladat**  Igaz vagy hamis az alábbi állítás?  ‘Az adatvédelemmel kapcsolatos vita új, a Facebook feltalálása után kezdődött’.  **2.feladat:**  Vitassa meg az adatvédelem kérdését családjával, barátaival, szomszédaival vagy kollégáival.  Mit tudott meg a saját értelmezése szerinti adatvédelemről és mások adatvédelemmel kapcsolatos látásmódjáról?  Emlékeztető: nézeteit posztolhatja a CSI-COP honlap fórumán: <https://csi-cop.eu/forum/>. A posztoláshoz regisztrálnia kell a honlapon egy log-in létrehozásával: <https://csi-cop.eu/citizenscientistlogin/> |
| A feladatok célja | Az *adatvédelemmel kapcsolatos különböző szempontok megértése*. |
| Rövid Tweet | Az internethez való mobil hozzáférés korában fontosabb szempont-e a kényelem, mint az adatvédelem? |

|  |  |
| --- | --- |
| **További olvasnivalók az 1. lépcsőhöz** | Az 1. lépcsőben említett további olvasnivalók megtalálhatók alább, az aláhúzott szövegre kattintva:  **Ajánlott olvasnivalók**  Lomas, N. (2021). *Answers being sought from Facebook over latest data breach*. Tech Crunch. Elérhető innen: <https://tcrn.ch/3xfrTsE>  Nayak, M. and Rosenblatt, J. (2021). *Google Must Face Suit Over Snooping on ‘Incognito’ Browsing*  Bloomberg Technology. Elérhető innen: <https://bloom.bg/3gFt4vV>  The Real Facebook Oversight Board Twitter account @FBoversight. Elérhető innen: <https://twitter.com/FBoversight>  **További olvasnivalók**  Guardian (2022). *John Oliver on Data Brokers: What they can buy is pretty troubling*. Guardian Culture. 11 April 2022: <https://bit.ly/3wzX0j3>  Holroyd, M. (2021). Ireland launches data protection inquiry into Facebook hack. *Euronews – Ireland*. Elérhető innen: <https://bit.ly/3mOfIOM>  Holvast, J. (2009). History of Privacy. In V. Matyáš et al. (Eds.): *The Future of Identity*, IFIP AICT 298, pp. 13–42, 2009. IFIP International Federation for Information Processing 2009. Megvásárolható a ResearchGate-en: <https://www.researchgate.net/publication/225802214_History_of_Privacy>  Nissenbaum, H. (2011). A Contextual Approach to Privacy Online. *Dædalus*, *Journal of the American Academy of Arts & Sciences*, Vol 140, No. 4 (Fall 2011), pp. 32-48. Elérhető innen: <https://www.amacad.org/publication/contextual-approach-privacy-online>  Sax, M. (2018). Privacy from an Ethical Perspective. Chapter in B. Van der Sloot & A. De Groot (Eds.), *The Handbook of Privacy Studies: An Interdisciplinary Introduction* (pp. 143-173). Amsterdam: Amsterdam University Press. Elérhető ezen a linken: <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3299047>  Warren, S.D. & Brandeis, L.D. (1890). The Right to Privacy*. Harvard Law Review*, Vol. 4, No. 5. (Dec. 15, 1890), pp. 193-220. Elérhető innen: [The Right to Privacy on JSTOR](https://www.jstor.org/stable/1321160?origin=crossref&seq=1#metadata_info_tab_contents) |

### 2. lépcső

|  |  |
| --- | --- |
| 2. lépcső címe: | Adatok és személyes adatok |
| Új ismeretek a 2. lépcsőben | 1: Az adatvédelem különböző szempontjainak leírása és megvitatása. |
| Téma | Mi a személyes adat? |
| Fő kérdés | *Miért érdekelne, hogy ki fér hozzá az adataimhoz, ha nincs rejtegetnivalóm?*  Kérdezze meg családját és barátait, hogy mit gondolnak az adataikról. Posztolhatja meglátásait a CSI-COP honlap fórumán: <https://csi-cop.eu/forum/>. Mielőtt posztol a fórumon, egy log-in létrehozásával regisztrálnia kell a honlapon: <https://csi-cop.eu/citizenscientistlogin/> |
| Rövid összefoglaló | Andreas Weigend (2017): “Minden alkalommal, amikor a Google-on keresünk valamit, a Facebook-on üzenünk valakinek, Uber-t használunk valahol vagy akár csak felkapcsolunk egy lámpát adatokat termelünk, melyeket a cégek gyűjtenek”.  [Lásd a további olvasnivalók részt a 2. lépcső végén] |
|  |  |
| Tananyag | **Mi az adat?**  Ismétlés: az 1. lépcsőben bemutatásra került az ‘adatvédelem’ koncepciója.  A CSI-COP informális tanfolyamának 2. lépcsőjében meg fogja érteni, hogy ‘mi az adat’, és azt, hogy ‘mely személyes adatai játszanak szerepet különböző szempontok szerint az Ön online életében: az online vásárlástól a barátokkal való üzenetváltásig és különböző információk kereséséig‘.  Az angol ‘data’ egyes száma datum:   * valaminek egyetlen *minősége* vagy *mennyisége*   A ‘data’ többes szám (több, mint egyetlen darab):   * Információs pontok, pédául *Önre vonatkozó adatok,* mint például   1. Ha Ön diák, akkor ‘hazai’ vagy nemzetközi diák   2. Születési idő   3. Az egyetemi felvételhez szükséges kvalifikáció   4. Állandó lakhely, egyetemi tartózkodás alatti lakhely   5. Telefonszám   Adatok mindenhol találhatók és számtalan formában tárolódnak:   * *Strukturálatlan:*   1. Nézze meg a YouTube videókat   2. Vizsgálja meg az Instagram képeket   3. Olvassa el az e-mail-eket   4. Műhold képek   5. Időjárási adatok * *Strukturált*   1. Diák/oktató azonosító szám – számsor   2. Társadalombiztosítási szám   3. Repülőjegy foglalás   structured vs. unstructured data  A fenti kép innen származik: <https://bit.ly/2PhkKHa>  A táblázat szövege:   |  |  |  | | --- | --- | --- | |  | **Strukturált adatok** | **Strukturálatlan adatok** | | **Jellemzők** | * Előre meghatározott adatmodellek * Általában csak szöveges * Könnyen kereshető | * Nincs előre meghatározott adatmodell * Lehet szöveg, kép, hang, videó, vagy egyéb * Nehezen kereshető | | **Hely** | * Relációs adatbázisok * Adattárházak | * Alkalmazások * NoSQL adatbázisok * Adattárházak * Adattavak | | **Ki generálja** | Emberek vagy gépek | Emberek vagy gépek | | **Jellemző alkalmazások** | * Légitársaságok foglalási rendszerei * Leltár kezelés * CRM rendszerek * ERP rendszerek | * Szövegszerkesztés * Prezentációs szoftverek * Email kliensek * Médiatartalmak megtekintésére és szerkesztésére szolgáló eszközök | | **Példák** | * Dátumok * Telefonszámok * TAJ számok * Hitelkártyák száma * Ügyfelek neve * Címek * Terméknevek és számok * Tranzakciós információk | * Szöveges fájlok * Jegyzőkönyvek * Email üzenetek * Hangfájlok * Videófájlok * Képek * Térfigyelő kamerák képei |   Irwin (2021) szerint: “Bizonyos körülmények között bármely a lentiek közül *személyes adat*nak tekinthető”:   * 1. Vezetéknév és keresztnév   2. Lakcím   3. E-mail cím   4. Személyi igazolvány szám   5. Tartózkodási hely   6. Internet Protocol (IP) cím   7. A telefonja hirdetési azonosítója   **A személyes adat olyan adat, amely egy “természetes” (élő) személyt azonosít.**    Pat Walshe a ‘**Privacy Matters’-**tőlazt mondja, hogy “A korábbiakhoz képest sokkal többet használjuk okostelefonunkat és számítógépünket hívásokra, személyes szövegek és képek küldésére, üzenetek továbbítására a WhatsAppon vagy a Snapchat-en keresztül, ételek vagy gyógyszerek online vásárlására, életünk személyes darabkáinak megosztására a közösségi médiában, egészségügyi (mentális vagy fizikális), politikai, vallási vagy utazási célú adatok keresésére, honlapok felkeresésére, visszajelzések hagyására, tetszésünk vagy nemtetszésünk kifejezésére. A digitális lét hatalmas mennyiségű, gyakran személyes jellegű vagy érzékeny adatot termel rólunk. Olyan adatokat, melyek lehetővé teszik, hogy mások jobban megismerjenek minket, mint mi saját magunkat” ([Privacy Matters](https://twitter.com/privacymatters?lang=en)).  **Önkéntesen megadhatunk adatokat**, amikor online rendelünk valamit vagy bejelentkezünk orvosi vizsgálatra. A rólunk szóló, eszközeinkre és online viselkedésünkre vonatkozó adatok **megszerezhetők és megfigyelhetők** (mint például a honlap, melyet meglátogattunk, a dal, amelyet meghallgattunk, a film, amelyet megnéztünk, az eszköz, amelyet használunk, tartózkodási helyünk – akár tudatában vagyunk ennek, akár nem). Adatokra lehet következtetni, ha profilt készítenek rólunk és analizálják a rólunk szóló információkat, mint például mely felhasználó hallgatott meg egy dalt vagy nézett meg egy filmet online, a dal vagy film kategóriája, mely ponton szakította meg a dalt vagy a filmet a személy, azzal a dátummal és időponttal együtt amikor megszakította, újraindította vagy abbahagyta a meghallgatást vagy megtekintést, a helyszín, ahol tartózkodott (legalább az ország) – adatok, melyek egyfajta digitalis árnyékát adják online tevékenységünknek ([Privacy Matters](https://twitter.com/privacymatters?lang=en)).  A személyes adatokon felül vannak **érzékeny személyes adatok**. Az európai általános adatvédelmi rendelet (GDPR) szerint - melyről a 4. lépcsőben fogunk többet tanulni – az **érzékeny személyes adatok** olyan adatokat foglalhatnak magukban, melyek elárulják:   * faji vagy etnikai származását * vallási meggyőződését * politikai véleményét * szakszervezeti tagságát.   Szintén érzékeny személyes adatok egy személy (mentális vagy fizikális) egészségére vonatkozó adatok; az egyén nemi életét vagy szexuális orientációját érintő adatok; a genetikai adatok; a biometrikus adatok (személyek egyedi azonosítására szolgáló adatok) valamint a büntetőügyi adatok ([Privacy Matters](https://twitter.com/privacymatters?lang=en)).  Brodkin (2021) 2021 áprilisában azt írta, hogy a T-Mobile:   1. “… egy új programot indít, mely felhasznál néhány, Önnel kapcsolatos adatot” 2. “*beleértve azon információkat, melyek leszűrhetők hálózati és eszközhasználati adataiból* (mint például a készülékére telepített app-ok)” 3. “és a termékeinkkel és szolgáltatásainkkal történő interakciókból saját magunk és harmadik felek hirdetései számára, hacsak Ön nem tiltja ezt meg számunkra ".   Hogyan érezné magát, ha a mobiltelefon szolgáltatója arról tájékoztatná, hogy a T-Mobile-hoz hasonlóan akar eljárni? Vagy ha Ön T-Mobile felhasználó, hogyan érez az adatgyűjtésre és adatfelhasználásra vonatkozó kijelentésükkel kapcsolatban?    A kép szövege:  **Az Ön digitális énje**  **Technikai azonosítók:**   * Süti ID-k * Mobil hirdetési ID * TV hirdetési ID * IP cím * Eszköz azonosítók (Bluetooth, WIFI, mobil sorozatszám, IMEI)   **Technikai információk:**   * Információk az eszközről – modell, operációs rendszer * Kapcsolat (WIFI, vezetékes, mobil hordozó) * Hely (GPS/WIFI/IP) * User agent – meghatározza a böngésző típusát, a telefon modelljét és az operációs rendszer verzióját   **Amit böngészik**  **Amit keres**  **Amit hallgat**  **Amit néz**  **Amit olvas**  **Ahol tartózkodik – pontosan, vagy megközelítőleg**  Mire számíthat a következő lépcsőkben?  A 3. lépcsőben megnézzük, hogy hogyan *követik adatainkat*.  A 4. lépcsőben megvizsgáljuk, hogy milyen *jogaink* vannak *adataink védelmére*.  A tanfolyam utolsó lépcsőjében, az 5. lépcsőben azokról az *online eszközökről* fogunk tanulni, melyeket *adataink hatékonyabb védelmére* használhatunk.  Ellenőrizze a tanultakat!  Kérem, ellenőrizze az alábbi kérdéssel és két feladattal, hogy mit tanult a 2. lépcsőben! |
| Ellenőrizze tudását | Mi a *személyes adat*? |
| Feladatok | **1.feladat: rövid teszt**  Az alábbiak közül mely név kapcsolódik a személyes adatokhoz?   * Leonardo da Vinci * Joe Biden elnök * Freddie Mercury * II. Erzsébet királynő * Alan Turing * Meghan Markle * Albert Einstein * A pápa * Kim Kardashian   A 2. lépcső 1. feladatára a választ a 3. lépcsőben fogja megtalálni.  **2.feladat**  Keressen és hallgasson meg TED beszédeket, például a Tech-szociológus, **Zeynap Tufekci** TED Global NYC beszédét (2017. szeptember):  ‘**We’re building a dystopia just to make people click on ads**’.  Emlékeztető: nézeteit posztolhatja a CSI-COP honlap fórumán: <https://csi-cop.eu/forum/>. A posztoláshoz regisztrálnia kell a honlapon egy log-in létrehozásával: <https://csi-cop.eu/citizenscientistlogin/> |
| A feladatok célja | Annak megértése, hogy mi a *személyes adat.* |
| Rövid Tweet | A kijelentés, hogy: “Nincs titkolnivalóm, ezért nem érdekel, hogy ki fér hozzá az adataimhoz” félreértelmezett. |

|  |  |
| --- | --- |
| **További olvasnivalók a 2. lépcsőhöz** | A 2. lépcsőben említett további olvasnivalók alább találhatók az aláhúzott szövegre kattintva:  **Ajánlott olvasnivalók**  Brodkin, J. (2021). *T-Mobile will sell your web-usage data to advertisers unless you opt o*ut.  arsTECHNICA. Elérhető innen: <https://bit.ly/3sUdkaQ>  Irwin, L. (2021). *Personal data vs. sensitive data: what’s the difference?* IT Governance. Elérhető innen: <https://bit.ly/3vhoRlX>  Privacy Matters on Twitter: @PrivacyMatters: <https://twitter.com/privacymatters?lang=en> |

### 3. lépcső

|  |  |
| --- | --- |
| 3. lépcső címe: | Online követési technológiák |
| Új ismeretek a 3. lépcsőben | 1. Az adatvédelem különböző szempontjainak leírása és megvitatása. 2. A személyes adatok gyűjtési módjának azonosítása és értékelése az interneten való szörfölés és az okos eszközök alkalmazásainak használata során. |
| Téma | Hogyan gyűjtik a személyes adatokat Internet használatunk során? |
| Fő kérdés | *Milyen kárt okozhatnak az online követési technológiák?*  Kérdezze meg családját és barátait, hogy mit gondolnak az adataikról! Posztolhatja meglátásait a CSI-COP honlap fórumán: <https://csi-cop.eu/forum/>. Mielőtt posztol a fórumon, egy log-in létrehozásával regisztrálnia kell a honlapon: <https://csi-cop.eu/citizenscientistlogin/> |
| Rövid összefoglaló | Nigel Warburton (2020): “A technológiai cégek az Ön engedélye nélkül gyűjtik adatait – tartózkodási hely, preferenciák, szokások, félelmek, betegségek, politikai nézetek – és ezeket megosztják egymás között”.  [Lásd a további olvasnivalók részt a 3. lépcső végén] |
|  |  |
| Tananyag | **Hogyan gyűjtik az Önre vonatkozó információt az interneten keresztül?**  Összefoglalva az előző két lépcsőben tanultakat:   * Az 1. lépcsőben bemutattuk az ‘adatvédelem’ koncepcióját. * A 2. lépcsőben megtanultuk, hogy a ‘személyes adat’ természetes (élő) személyre vonatkozik.   Ebben a lépcsőben azokról az online eszközökről fogunk tanulni, amelyek az adatokat gyűjtik, miközben az internetet használjuk.  Eliza Crawford termékmenedzser (2020) arról tájékoztat minket, hogy az internet használat során történő **adatgyűjtés célja az, hogy megtudják, hogyan viselkedünk, ha felkeresünk egy honlapot.** Vagyis **“betekintést nyernek abba, hogy az ügyfelek hogyan használják” a honlapokat, “annak érdekében, hogy személyre szabott online élményt nyújtsanak, és célzott hirdetésekkel vásárlásra bírják a felhasználót.”**  Crawford (2020) a következőket mondja az online követés használatának magyarázataként:   * “Ha egy éttermet keres a Google-on és a szolgáltatás a környezetében lévő vendéglők listáját adja meg, ez azért történik, mert a keresőmotor ismeri az Ön tartózkodási helyét.” * “Ha egy e-bolt termékeket ajánl az Ön számára, ez azért van, mert a korábban megtekintett vagy megvásárolt árucikkek követése révén tudja, hogy Ön mit szeret.”   Pat Walshe (Privacy Matters) emlékeztet minket, hogy a **viselkedési adatok** a következőket foglalhatják magukban:   * Az Ön **internet böngészési** adatait – meglátogatott honlapok, a látogatás időpontja, az ország, ahonnan a keresés történt (az IP címből következtetve – amely egy egyedi karaktersor, mely azonosít minden, az internethez csatlakoztatott eszközt, és ez az adat automatikusan elküldésre kerül, amikor Ön meglátogat egy honlapot). Azt is vegye figyelembe, hogy amikor elhagy egy honlapot, akkor megtudják, hogy utána mely honlapot látogatja meg, és a következő honlap tudni fogja, hogy mely honlapról érkezett. Mindezeket internet böngészési adatnak tekintik. * ‘**Kattintási viselkedés’** – a személynek a honlappal való interakciójára vonatkozó adatok, amelyek magukban foglalhatják, hogy mire kattint, görget vagy mit érint meg az érintőképernyőn. * ‘**Keresőmotorok’,** mint a Google, mely gyűjthet és felhasználhat adatokat arról, hogy Ön mit keresett, milyen eredményekre kattintott, mi az IP címe, és egyedi süti azonosítót használhat az Ön követésére. * **Tartózkodási hely** – a meglátogatott hely helyszíne és típusa (szupermarket, kaszinó, vallásgyakorlási hely, kórház), egy app használatának helyszíne, utazásának időpontja, útvonala, a látogatások vagy utazások gyakorisága. A tartózkodási helyre vonatkozó adatok nagyon [árulkodóak](https://www.fastcompany.com/3068846/how-your-location-data-identifies-you-gilad-lotan-privacy) lehetnek és a viselkedésre utalhatnak. * **Vásárlási előzmények** – ezek magukban foglalhatják az előfizetések típusát (szakszervezeti tagság, fitness, újságok,stb.), a hotel vagy éttermi foglalásokat, amelyeket [keresést, térképeket, okos asszisztenseket](https://myaccount.google.com/purchases?pli=1) használva, közvetlenül viszonteladó révén vagy harmadik fél szolgáltatón keresztül tettünk, stb. * **Fizetési vagy ‘**[tranzakciós’](https://medium.com/the-capital/what-you-dont-know-about-transactional-privacy-but-you-should-d0072941d050) **adatok** – kifizetések, amelyek megmutatják, hogy kinek vagy mely szervezetnek fizetett (elárulhatják a szervezet típusát – orvosi rendelő, gyógyszertár, szeszes ital vagy étel forgalmazó, könyvesbolt, stb.) mennyit, mikor és milyen gyakran. Jó példa az érintőkártyás fizetés – gondoljon a kávéra, amelyet az utazása kezdetén vesz meg, a fizetés helyére és idejére, majd azokra a kifizetésekre, amelyeket ugyanazon kártyával a nap során végez. * **Média streamelés** – “[you are what you stream](http://assets.ctfassets.net/ziwa9xqm84y1/CFPSdMWTrtrhdD8iVHIcy/b136bd5e622c52675ec7e0b7dbde4625/Spotify_Media_Kit_2018_-_CA.pdf)” és “[They know what You Watched Last Night](https://www.nytimes.com/2019/10/25/business/media/streaming-data-collection-privacy.html)”. A média streamelés **sok** viselkedési adatot generál a következőkről:   + a streaming zene, audio vagy TV/film szolgáltatáshoz való hozzáférés időpontja és a hozzávetőleges helyszín (ország vagy régió szint) ahonnan ez történt,   + mely felhasználói profil kereste meg és használta a szolgáltatást (név + kategória, pl. gyermek),   + a zene, hangoskönyv, TV/film (pl. politikai horror, felnőtt tartalom) kategóriája,   + tartalomkeresés,   + szüneteltetett-e egy dalt vagy filmet és mennyi ideig (beleértve az időponto(ka)t),   + átugrotta-e vagy abbahagyta-e egy dal vagy egy TV sorozat epizódjának meghallgatását,   + megosztott-e tartalmat és kivel, valamint voltak-e interakciói más felhasználókkal a szolgáltatáson belül,   + értékelt-e dalt, TV műsort vagy filmet,   + lejátszási listák vagy ‘megnézendő’ listák, melyeket készít,   + a szolgáltatás igénybevételéhez használt eszköz, annak IP címe és azonosítói. * **Aktivitási/egészségügyi adatok** – adatok az aktivitási appok használatáról, mint pl. biciklizés, futás, sétálás, vagy adatok az Ön egészségéről a diétás vagy termékenységi appokon keresztül. Ezek az adatok nagyon árulkodóak lehetnek, és gyakran kapcsolódnak például a tartózkodási helyhez. * **Közösségi media grafikon –** adatok, melyek a személyek közötti kapcsolati hálót mutatják, azok természetét és a kommunikáció mintáját.   Ghostery (2017) tanulmánya szerint “globálisan a honlapok (egyedi domének) legalább 79 százalékában vannak jelen olyan követők, amelyek adatokat gyűjtenek az internet használók online viselkedéséről. Az internetes követés olyannyira mindent átható lett, a honlapok kb. 10 százaléka tíz vagy több cégnek küldi el a gyűjtött adatokat (egyedi követő domének). Az internetes forgalom szempontjából a honlap oldalak 15 százalékát legalább *tíz vagy több* követő monitorozza. A tanulmány szerint a Google (oldaltartalmak 60.3 százaléka) és Facebook (27.1 százalék) követési forgatókönyvek a legelterjedtebbek”.  **A picture containing dark  Description automatically generated**  Ezt a követést digitális eszközökkel végzik:  A tanfolyam 1. lépcsőjében már találkoztunk a sütikkel John Oliver 2022. április 10-i „Last Week Tonight” című HBO-műsora kapcsán, amely leleplezte az adatbrókereket.   1. **Sütik**: A sütik kis adatdarabok, melyeket a honlapok a felhasználó eszközén tárolnak. A honlapok gyakran **használnak sütiket,** hogy **emlékezzenek a felhasználói preferenciákra,** és **személyre szabott élményt nyújtsanak,** valamint **információt gyűjtsenek hirdetési célokra.** Amint egy honlap sütit helyezett el a felhasználó számítógépén, a süti tulajdonosa bármikor elérheti azt. Így a honlapok használhatják a sütiket a felhasználók laptól-lap vagy weboldatól-weboldal követésére. A süti típusától függ, hogy mennyi ideig tudja a süti követni a felhasználót. Például munkamenet sütik, állandó, elsődleges, és harmadik féltől származó sütik (Crawford, 2020). 2. **Ujjlenyomat**: Az ujjlenyomatos követés a honlap követés egyik formája, amely a felhasználó **eszközének vagy böngészőjének jellemzőit használja egy felhasználói profil létrehozására**. Az ujjlenyomatos követés a következő információkat használja: használt eszköz, az azon futó operációs rendszer, képernyő felbontása, böngésző és annak verziója, nyelv, időzóna. Crawford (2020) szerint: “Önmagában egyik információdarabka sem értékes. De, amikor mindet összerakják, akkor hihetetlenül pontosan tudja azonosítani a felhasználót. Az **Electronic Frontier Foundation** ([EFF](https://www.eff.org/)) futtat egy honlapot (‘[cover your tracks](https://coveryourtracks.eff.org/)’), amely teszteli a böngészőjét, hogy megmutassa milyen egyedi az Ön ujjlenyomata más követett helyekhez képest.” 3. **E-mail követés**: Az e-mail követő **szoftver képzeletbeli képpixelt helyez el az e-mailekben, mely érzékelni tudja az időpontot, amikor megnyitotta az e-mail-t.** Az e-mail követés célja, hogy a cégek/viszonteladók időt takarítsanak meg, és megtudják, hogy a cég első e-mail-je elég érdekes volt-e az Ön számára, hogy megnyissa. Ha nem, akkor valószínűtlen, hogy további, követő e-mail-eket meg fog nyitni. A felesleges követő e-mail-ek megelőzése révén az e-mail követés időt takarít meg mind a kereskedelmi ügynök, mind az e-mail címzettje számára. Hasonlóképpen, ha egy cég észleli, hogy a címzett rákattint a küldött linkre, és elolvassa a kísérőlevelet vagy a mellékelt ajánlatot, akkor a cég tudja, hogy Ön az érdeklődésük középpontjában van. Ha abban a pillanatban keresik meg Önt, amikor a cég ajánlatára gondol (pl. egy ruhanemű vásárlására), sokkal aktuálisabb lesz a megkeresés a cég/viszonteladó számára.   Sivan-Sevilla és társai (2020) tanulmánya azt találta, hogy “olyan cégek, amelyekről még sohasem hallottunk, adatpontokat gyűjtenek életünk minden vonatkozásáról – érdeklődési körünkről, vásárlásainkról, egészségi állapotunkról, tartózkodási helyünkről és másokról”. IAB (2019, amit Sivan-Sevilla és társai cikkében, 2020 idéz) “Ezeket az adatpontokat azután kivételesen leleplező viselkedési profilokká összesítik, felfedve személyiségünk intim részleteit, és táplálva a multi-milliárd-dolláros hirdetési ipart, amely állítólag meg tudja jósolni, hogy mit szeretnénk venni, hogy célzott hirdetésekkel bombázhassanak”.  Sivan-Sevilla és társai (2020) továbbá azt írják, hogy amikor a hirdetők összevetik a felhasználók egészségügyi problémáira, oktatási érdeklődésére és új fogyasztási szokásaira vonatkozó információkat sokkal jobb helyzetbe kerülnek annak megítélésében, hogy egy felhasználó mikor tehető fogyasztóvá, és mikor fog olyan vásárlási döntéseket hozni, amelyeket a hirdetők más módon nem tudtak volna előre látni. Tanulmányok bemutatták, hogy a különböző honlapokról származó adatokat hogyan összesítik, és azokból hogyan következtetnek a felhasználók célcsoportjaira és érdeklődésére, manipulálva őket, hogy a “helyes” (személyre szabott) hirdetésre kattintsanak a “helyes” (személyre szabott) időpontban. A hirdetési ipar ezeket a pillanatokat “**a fogyasztók elsőrendű érzékenységi pillanataként**” definiálta…amikor a felhasználók ‘kivételesen fogékonyak’…”.  Srinivasan (2020) megvilágítja, hogy: “Az elektronikus hirdetési ipar felemelkedése, amelyet ma széles körben “programozott hirdetésnek” neveznek, párhuzamosan történt az elektronikus kereskedés fellendülésével a gazdaság különböző szektoraiban… a **Right Media,** az egyik első hirdetési technológiai cég indította el az **RMX** “hirdetési csereüzletet,” amely a **legelső elektronikus kereskedési felület volt hirdetések számára**. ... Ma a **Google** egyeduralkodóként egyidejűleg működik a csere vezetői és közvetítői minőségében, amelyet a kiadóknak és hirdetőknek használniuk kell … A Google nemcsak elad harmadik fél honlapokhoz tartozó hirdetési felületeket, hanem a saját oldalain (Google Search and YouTube) megjelenő hirdetési felületeket is értékesíti”.  Srinivasan (2020) szerint “A hirdetési üzlet drasztikusan megváltozott az elmúlt két évtizedben. Manapság az online hirdetésekről, amelyek a hirdetések legnagyobb kategóriáját adják ritkán tárgyalnak emberek. A technológiai fejlődés lehetővé teszi, hogy hirdetési felületeket nagy sebességgel, elektronikusan adjanak és vegyenek központi kereskedelmi helyszíneken keresztül, személyes találkozások nélkül. Amikor egy felhasználó felkeres egy honlapot a lapon lévő hirdetési felület azonnal egy vagy több ilyen helyszínre irányít. Itt a felületet a legtöbbet kínáló szerezheti meg valós időben. Ezen aukciók eredményeképpen a hirdetések visszatérnek az eredeti honlapra, és időben betöltődnek a felhasználó számára, anélkül, hogy bármit észrevenne. A felhasználó csak a neki szánt hirdetést látja, pl. a Barclays bankét.”  Most már érthető, hogy egyre több adatot elfognak, megfigyelnek és következtetésekre használnak azok, akikkel Ön közvetlen kapcsolatban van, ezáltal nemcsak az Ön által kért alapszolgáltatást, hanem egyre inkább ‘személyre szabott élményeket’ nyújtanak, akár kérte, akár nem, és célzott hirdetéseket küldenek honlapjaikon, appjaikon és szolgáltatásaikon keresztül. De adatait nemcsak azok fogják el, figyelik meg és használják következtetésekre, akikkel közvetlen kapcsolatban van, hanem a hirdetési közegben működő harmadik felek is, amelyek be lehetnek ágyazva az Ön által meglátogatott honlapokba vagy használt appokba, azért, hogy megcélozhassák például [viselkedésalapú hirdetésekkel](https://fil.forbrukerradet.no/wp-content/uploads/2020/01/2020-01-14-out-of-control-final-version.pdf). Adatait arra is használhatják, hogy kövessék az interneten és az appokon keresztül célzott elérés érdekében, mint amilyen például a [valós idejű licit](https://www.outbrain.com/blog/programmatic-advertising/), amely lehetővé teszi a hirdetők számára, hogy automatikusan, valós időben licitáljanak bizonyos személyek elérésére specifikus jellemzők szerint – például korcsoport, nem, mobil eszköz vagy helyszín.  Tehát az ÖNre vonatkozó adatok nagyon személyesek lehetnek, amelyek életének intim vonatkozásait fedik fel. Olyan módon lehet hatásuk, melyre sohasem gondolt, sértik az adatvédelemmel kapcsolatos elvárásait, és nincsenek tekintettel magánéletének védelmére. Például a Grindr app-pal kapcsolatban azt [találták](https://fil.forbrukerradet.no/wp-content/uploads/2020/01/2020-01-14-out-of-control-final-version.pdfhttps:/fil.forbrukerradet.no/wp-content/uploads/2020/01/2020-01-14-out-of-control-final-version.pdf), hogy profilozásban és hirdetésben érdekelt “*nagy számú harmadik féllel*” oszt meg információt. A megosztott adatok között szerepelt az “*IP cím, hirdetési azonosító, GPS szerinti helyzet, kor és nem*.” A norvég adatvédelmi hatóság vizsgálatot indított az ügyben, és [megbüntette](https://www.theguardian.com/technology/2021/jan/26/grindr-fined-norway-sharing-personal-information) a Grindr céget 100 millió koronára.  Minden, a fentiekben említett adat személyes adat, amelyet az adatvédelmi törvények védenek, mint például a GDPR és az EU elektronikus adatvédelmi törvénye (az [ePrivacy Directive](https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A02002L0058-20091219) ‘ePD’), amelyet a CSI-COP informális tanfolyamának következő lépcsőjében (4. lépcső) fogunk megbeszélni. Ezek a törvények követelményeket támasztanak a magánszektor és a közszféra azon intézményei számára, amelyek Önre vonatkozó adatokat fognak el, figyelnek meg és következtetéseket vonnak le azokból, és meghatározzák a felhasználással kapcsolatos jogokat. Ezeket megint csak a tanfolyam 4. lépcsőjéban fogjuk megbeszélni.  Tartson egy perc szünetet, és gondolja át, hogy adatai mit árulnak el ÖNről és hozzátartozóiról.  Azt is vegye figyelembe, hogy az ‘ingyenes’ Wifi használata során is adatokat kell megadnia magáról, hogy elérje az internetet. Az alábbi ábra mutatja, hogy milyen adatok kerülnek összegyűjtésre.    A kép szövege:  **“Ingyenes” Wifi**  **Fiókadatok**   * Név * Születési idő * Nem * Levelezési cím * Mobiltelefonszám * Email cím * Az eszköz MAC azonosítója   **Felhasználási adatok**   * Pl. a WiFi használat ideje és a hotspot helye * Egyéb, szolgáltatáshoz kötődő adatok, beleértve az IP címet és az eszközzel kapcsolatos információkat   **Emlékeztető adatok**   * **E**lső háziállat neve * Anya lánykori neve * Kedvenc hely   Az ingyenes WiFi (és hirdetési partnereink) felhasználhatják az Ön fiók- és felhasználási adatait, hogy személyre szabott reklámot küldjenek Önnek, többek között sütikkel. Ha további információt szeretne, vagy változtatni kíván ezen, kattintson az alábbi Ingyenes Wifi Hirdetési Opciókra.   * Az ingyenes WiFi (és hirdetési partnerei) felhasználhatják az adataimat, hogy személyre szabott reklámot küldjenek. * Az ingyenes WiFi megoszthatja személyes adataimat a TV Limited-del, hogy a TV Limited számomra relevánsabb hirdetéseit láthassam.   Mire számíthat a következő lépcsőkben?  A 4. lépcsőben megvizsgáljuk, hogy milyen *jogaink* vannak *adataink védelmére*.  A tanfolyam utolsó lépcsőjében, az 5. lépcsőben azokról az *online eszközökről* fogunk tanulni, melyeket *adataink hatékonyabb védelmére* használhatunk.  Ellenőrizze a tanultakat!  Kérem, ellenőrizze, hogy mit tanult a 3. lépcsőben! A 2. lépcső 1. feladatának megoldását a jelen lépcső két feladata tartalmazza. |
| Ellenőrizze tudását | Milyen típusai vannak a sütiknek?  Mi a digitális ujjlenyomat?  Hogyan működik az E-mail követés? |
| Feladatok | **Válasz a 2. lépcső 1. feladatára**  A 2. lépcső 1. feladatában személyes adatokat kellett azonosítani egy neveket tartalmazó listából. Mivel a személyes adatok csak természetes (élő) emberekre vonatkoznak azon személyek neve, akik már nem élnek nem személyes adatok. Jól gondolta? Ellenőrizze az alábbiakban:   * Leonardo da Vinci – nem személyes adat * Joe Biden elnök * Freddie Mercury – nem személyes adat * II. Erzsébet királynő * Alan Turing – nem személyes adat * Meghan Markle * Albert Einstein – nem személyes adat * A pápa (ez nem teljesen egyértelmű: mivel a jelenlegi, élő pápára vonatkozik, személyes adatnak tekinthető) * Kim Kardashian     **3. lépcső 1. feladat**   * 1. Keressen az interneten különböző fajta sütiket, amelyek be lehetnek ágyazva honlapokba!   2. Mi a különbség az ujjlenyomatos és az e-mail követés között?   **3. lépcső 2. feladat**  Vitassa meg családjával, barátaival, szomszédaival vagy kollégáival, hogy mit értenek ‘***online behaviour profiling***’ alatt, és hogyan működik ez az interneten.  **3. lépcső 3. feladat**  Próbálja ki az alábbi ingyenes online játékkal, hogy el tudja-e kerülni a sütiket:  <https://cookieconsentspeed.run/>    Emlékeztető: nézeteit posztolhatja a CSI-COP honlap fórumán: <https://csi-cop.eu/forum/>. A posztoláshoz regisztrálnia kell a honlapon egy log-in létrehozásával: <https://csi-cop.eu/citizenscientistlogin/> |
| A feladatok célja | Ismeretek szerzése a viselkedési profilozásról |
| Rövid Tweet | Követési technológiák |

|  |  |
| --- | --- |
| **További olvasnivalók a 3. lépcsőhöz** | A 3. lépcsőben említett további olvasnivalók alább találhatók az aláhúzott szövegre kattintva:  **Ajánlott olvasnivalók**  Crawford, E. (2020). Website Tracking: Why and How do Websites Track you? CookiePro Blog: Cookie Compliance. Elérhető innen: <https://www.cookiepro.com/blog/website-tracking/>  EFF (no date). The Electronic Frontier Foundation. The leading non-profit defending digital privacy, free speech, and innovation [for 30 years and counting!](https://www.eff.org/tags/eff30) Elérhető innen: <https://www.eff.org/>  Ghostery (2017). 79 Percent of Websites Globally Are Secretly Tracking Your Personal Data. Ghostery. Elérhető innen: <https://www.ghostery.com/press/ghostery-global-tracking-study/>  Privacy Matters on Twitter: @PrivacyMatters: <https://twitter.com/privacymatters?lang=en>  **További olvasnivalók**  Sivan-Sevilla, I., Chu, W., Liang, X. and Nissenbaum, H. (2020). Unaccounted Privacy Violation: A Comparative Analysis of Persistent Identification of Users Across Social Contexts. Federal Trade Commission (FTC) PrivacyCon 2020. A cikk elérhető a következő linken: <https://news.cornell.edu/stories/2020/06/study-online-trackers-follow-health-site-visitors>  Srinivasan, D. (2020). Why Google Dominates Advertising Markets Competition Policy Could Lean on the Principles of Financial Market Regulation. 24 STAN. TECH. LAW REV. Elérhető innen: <https://law.stanford.edu/publications/why-google-dominates-advertising-markets/>  Warburton, N. (2020) inside cover of book by Véliz, C. (2020). Privacy is Power: Why and how you should take back control of your data. Penguin Hardback. |

4. lépcső

|  |  |
| --- | --- |
| 4. lépcső címe: | Az adatvédelemmel kapcsolatos jogok |
| Új ismeretek a 4. lépcsőben | 1. Az adatvédelem különböző szempontjainak leírása és megvitatása. 2. A személyes adatok gyűjtési módjának azonosítása és értékelése az interneten való szörfölés és az okos eszközök alkalmazásainak használata során. 3. Az adataink védelmét biztosító egyezményekből eredő adatvédelmi jogok megértése. |
| Téma | Az adatvédelemmel kapcsolatos jogok: ENSZ emberi jogok egyetemes nyilatkozata (UN Charter on Human Rights); Európai Unió Alapjogi Chartája (EU Charter on Human Rights); Általános adatvédelmi rendelet (GDPR) |
| Fő kérdés | *Milyen jogaim vannak az adatvédelemmel kapcsolatban?*  Kérdezze meg családját és barátait, hogy mit gondolnak az adataikról. Posztolhatja meglátásait a CSI-COP honlap fórumán: <https://csi-cop.eu/forum/>. Mielőtt posztol a fórumon, egy log-in létrehozásával regisztrálnia kell a honlapon: <https://csi-cop.eu/citizenscientistlogin/> |
| Rövid összefoglaló | Az emberi jogokkal kapcsolatos adatvédelmi jogszabályok és rendeletek |
|  |  |
| Tananyag | **Az adatvédelem joga**  Összefoglalva az előző három lépcsőben tanultakat:   * Az 1. lépcsőben bemutattuk az ‘adatvédelem’ koncepcióját. * A 2. lépcsőben megtanultuk, hogy a ‘személyes adat’ természetes (élő) személyre vonatkozik. * A 3. lépcsőben azokról a módszerekről tanultunk, melyekkel adatainkat elfogják online (pl. cookie-k segítségével).   Ebben a lépcsőben az ‘emberi jogokat’ fogjuk megvizsgálni.  Pat Walshe, a Privacy Matters munkatársa arra emlékeztet minket, hogy „az emberi jogok régóta fontosnak számítanak. Nagy-Britanniában például [1689](https://www.webarchive.org.uk/wayback/archive/20131031165954/http:/www.bl.uk/onlinegallery/takingliberties/staritemshumanrights.html) óta az emberi jogokat nélkülözhetetlennek tekintették az emberi lét, méltóság és az alapvető jogok és szabadság védelme szempontjából (British Library, 2013). A jogok és a szabadság ma életünk különböző dimenzióit alakítják – offline és online. Kezdve a véleményszabadságtól a kapcsolati és gyülekezési jogig, a vallásszabadságig, az oktatáshoz való jogig, az igazságos elbírálás jogáig, a házasodási jogig és az **adatvédelemhez való jog**ig. Az emberi jogok számítanak. Minden nap. Offline és online. Ezek teszik lehetővé, hogy emberi lényként létezzünk.”  A modern korban az emberi jogok **1948**-ban tettek szert globális fontosságra. A II. világháború során elkövetett atrocitásokra adott válaszként az ENSZ Közgyűlése elfogadta az [Emberi Jogok Egyetemes Nyilakozatát](https://eur01.safelinks.protection.outlook.com/?url=https%3A%2F%2Fwww.un.org%2Fen%2Fabout-us%2Funiversal-declaration-of-human-rights&data=04%7C01%7Cab7778%40coventry.ac.uk%7Ccb9af077aa24412296d008d8f1357e72%7C4b18ab9a37654abeac7c0e0d398afd4f%7C0%7C0%7C637524559344161263%7CUnknown%7CTWFpbGZsb3d8eyJWIjoiMC4wLjAwMDAiLCJQIjoiV2luMzIiLCJBTiI6Ik1haWwiLCJXVCI6Mn0%3D%7C1000&sdata=uA%2B1stRDQLrowoxPVHRcaPjHo%2B0BT4CK0n60J364GWA%3D&reserved=0) (Universal Declaration of Human Rights - **UDHR**) a minden ember számára járó alapvető jogok védelmére. Az UDHR 12. paragrafusa védelmet biztosít egy személy **magánéletével, családjával, otthonával** és **levelezésével** kapcsolatos önkényes beavatkozásokkal szemben.  1949-ben néhány európai ország megalapította az [Európa Tanácsot](https://eur01.safelinks.protection.outlook.com/?url=https%3A%2F%2Fwww.coe.int%2Fen%2Fweb%2Fyerevan%2Fthe-coe%2Fabout-coe%2Foverview&data=04%7C01%7Cab7778%40coventry.ac.uk%7Ccb9af077aa24412296d008d8f1357e72%7C4b18ab9a37654abeac7c0e0d398afd4f%7C0%7C0%7C637524559344161263%7CUnknown%7CTWFpbGZsb3d8eyJWIjoiMC4wLjAwMDAiLCJQIjoiV2luMzIiLCJBTiI6Ik1haWwiLCJXVCI6Mn0%3D%7C1000&sdata=JYIiQpLG0k8JcNGCurBcULLRd2iAd9iwASOg9yPWVOg%3D&reserved=0) (**ET,** Council of Europe - **CoE**), amely napjainkban 47 tagországot egyesít. **1950**-ben az Európa Tanács elfogadta az [Emberi Jogok Európai Egyezményét](https://eur01.safelinks.protection.outlook.com/?url=https%3A%2F%2Fwww.echr.coe.int%2FPages%2Fhome.aspx%3Fp%3Dbasictexts%26c%3D&data=04%7C01%7Cab7778%40coventry.ac.uk%7Ccb9af077aa24412296d008d8f1357e72%7C4b18ab9a37654abeac7c0e0d398afd4f%7C0%7C0%7C637524559344171219%7CUnknown%7CTWFpbGZsb3d8eyJWIjoiMC4wLjAwMDAiLCJQIjoiV2luMzIiLCJBTiI6Ik1haWwiLCJXVCI6Mn0%3D%7C1000&sdata=iickwfKhNhJyIxTdU3hZDPYgAeUvGbj0RG1KkT7fPBE%3D&reserved=0) (European Convention on Human Rights - ECHR), annak érdekében, hogy ez a jövőben megvédje a polgárokat a II. világháborúban elkövetett atrocitásokhoz hasonló bűncselekményektől. Az ECHR az UDHR-hez hasonló alapvető jogokat tartalmaz, és **1953**-ban lépett hatályba.AzECHR az első olyan **nemzetközileg kötelező jogi eszköz**, amely az emberi jogokat védi. Megjegyzendő, hogy az Európai Unió (EU) mindegyik tagországa [csatlakozott](https://eur01.safelinks.protection.outlook.com/?url=https%3A%2F%2Fwww.europarl.europa.eu%2Ffactsheets%2Fen%2Fsheet%2F146%2FEuropean-Union-Charter&data=04%7C01%7Cab7778%40coventry.ac.uk%7Ccb9af077aa24412296d008d8f1357e72%7C4b18ab9a37654abeac7c0e0d398afd4f%7C0%7C0%7C637524559344171219%7CUnknown%7CTWFpbGZsb3d8eyJWIjoiMC4wLjAwMDAiLCJQIjoiV2luMzIiLCJBTiI6Ik1haWwiLCJXVCI6Mn0%3D%7C1000&sdata=SSGYaHq2HZqUFPSYw%2FxwiNv5P40SeiL0jSwvhBgrIgU%3D&reserved=0) az ECHR-hez.  Az ECHR 8. paragrafusa kimondja, hogy mindenkinek joga van arra, hogy **magán- és családi életét, otthonát** és **levelezését** tiszteletben tartsák. Könnyű megérteni, hogy ez a jog hogyan védi egy személy életének intim vonatkozásait, azokat a vonatkozásokat, amelyeket könnyű online megfigyelni.  Az ECHR 8. paragrafusa a magánélethez való jogunkat védi, de ugyanakkor az adatvédelemre is vonatkozik, mivel a személyekre vonatkozó információ használata nemcsak az emberek magánéletére, hanem más jogaira és szabadságára is kihatással van, ahogy a tanfolyam ezt be fogja mutatni. 1981-ben az **ET** számos, a személyes információk kezelésére vonatkozó irányelvet és szabályt fogadott el, annak érdekében, hogy védelmet biztosítson a polgároknak, jogaiknak és szabadságuknak, különös tekintettel az adatvédelemre. Ezek az irányelvek és szabályok 108-as Nyilatkozat néven ismertek. A Nyilatkozatot nemrégiben megújították, hogy tükrözze azokat a technológiai és adathasználati változásokat, melyek károsan befolyásolhatják az emberi jogokat. Ez a dokumentum [108+ Nyilatkozat](https://eur01.safelinks.protection.outlook.com/?url=https%3A%2F%2Fwww.coe.int%2Fen%2Fweb%2Fdata-protection%2Fconvention108%2Fmodernised&data=04%7C01%7Cab7778%40coventry.ac.uk%7Ccb9af077aa24412296d008d8f1357e72%7C4b18ab9a37654abeac7c0e0d398afd4f%7C0%7C0%7C637524559344181176%7CUnknown%7CTWFpbGZsb3d8eyJWIjoiMC4wLjAwMDAiLCJQIjoiV2luMzIiLCJBTiI6Ik1haWwiLCJXVCI6Mn0%3D%7C1000&sdata=4%2FyHZ6SiuxCw1AEWj0hVH0gYqGJA%2FbRQxow2%2F1Fazw0%3D&reserved=0) (Convention 108+) néven ismert.  **2000**-ben az EU létrehozta az [Alapjogi Chartát](https://eur01.safelinks.protection.outlook.com/?url=https%3A%2F%2Ffra.europa.eu%2Fen%2Feu-charter&data=04%7C01%7Cab7778%40coventry.ac.uk%7Ccb9af077aa24412296d008d8f1357e72%7C4b18ab9a37654abeac7c0e0d398afd4f%7C0%7C0%7C637524559344181176%7CUnknown%7CTWFpbGZsb3d8eyJWIjoiMC4wLjAwMDAiLCJQIjoiV2luMzIiLCJBTiI6Ik1haWwiLCJXVCI6Mn0%3D%7C1000&sdata=EWVDDZrcKGqL9KAMEwfgIVTWdQXjtz5dIRfobjVTtkk%3D&reserved=0) (Charter of Fundamental Rights - **EU CFR**). A charta 2009-ben vált törvényileg kötelezővé az EU tagországaiban. Az ECHR-hez hasonlóan az EU Alapjogi Chartája kimondja, hogy mindenkinek joga van arra, hogy magán- és családi életét, otthonát és közléseit tiszteljék (7. paragrafus). Továbbá az **EU CFR** azt is elrendeli, hogy mindenkinek joga van személyes adatainak védelmére (8. paragrafus).  Az EU CFR 7. és 8. paragrafusa megkülönbözteti a magánélethez való jogot és az adatvédelemhez való jogot. Ezeket a jogokat az **EU** [ePrivacy Directive](https://eur01.safelinks.protection.outlook.com/?url=https%3A%2F%2Feur-lex.europa.eu%2FLexUriServ%2FLexUriServ.do%3Furi%3DOJ%3AL%3A2009%3A337%3A0011%3A0036%3Aen%3APDF&data=04%7C01%7Cab7778%40coventry.ac.uk%7Ccb9af077aa24412296d008d8f1357e72%7C4b18ab9a37654abeac7c0e0d398afd4f%7C0%7C0%7C637524559344181176%7CUnknown%7CTWFpbGZsb3d8eyJWIjoiMC4wLjAwMDAiLCJQIjoiV2luMzIiLCJBTiI6Ik1haWwiLCJXVCI6Mn0%3D%7C1000&sdata=4Vp99U43lyhjPuhTxYvnTnt81EYIefMk6pnaMHYdfEE%3D&reserved=0) néven ismert **e-adatvédelmi eszköze** (amely a sütikre és más online követési eszközökre vonatkozik), valamint az európai [Általános Adatvédelmi Rendelet](https://eur01.safelinks.protection.outlook.com/?url=https%3A%2F%2Feur-lex.europa.eu%2Flegal-content%2FEN%2FTXT%2F%3Furi%3DCELEX%3A02016R0679-20160504%26qid%3D1532348683434&data=04%7C01%7Cab7778%40coventry.ac.uk%7Ccb9af077aa24412296d008d8f1357e72%7C4b18ab9a37654abeac7c0e0d398afd4f%7C0%7C0%7C637524559344191125%7CUnknown%7CTWFpbGZsb3d8eyJWIjoiMC4wLjAwMDAiLCJQIjoiV2luMzIiLCJBTiI6Ik1haWwiLCJXVCI6Mn0%3D%7C1000&sdata=7C%2FTUWAp1ZxSTjmU2iVp1YX%2FPgDRUVzbcGrR4s2Bg6A%3D&reserved=0) (General Data Protection Regulation - **GDPR**) lépteti hatályba. Az EU és az **ET** [adatvédelmi szabályait](https://eur01.safelinks.protection.outlook.com/?url=https%3A%2F%2Fec.europa.eu%2Finfo%2Flaw%2Flaw-topic%2Fdata-protection%2Feu-data-protection-rules_en&data=04%7C01%7Cab7778%40coventry.ac.uk%7Ccb9af077aa24412296d008d8f1357e72%7C4b18ab9a37654abeac7c0e0d398afd4f%7C0%7C0%7C637524559344191125%7CUnknown%7CTWFpbGZsb3d8eyJWIjoiMC4wLjAwMDAiLCJQIjoiV2luMzIiLCJBTiI6Ik1haWwiLCJXVCI6Mn0%3D%7C1000&sdata=rR73YvtoWbmgl7AbuGa3PBQSGq43G4KIic1IymmNfSU%3D&reserved=0) a tagországok jogrendszere hajtja végre, és azokat meg is erősítették a technológiában és az adathasználatban történt változások figyelembevételével. Manapság, amikor az emberek a mobiltelefonjaikat vagy laptopjaikat használják a személyekre vonatkozó adatokat valós időben lehet gyűjteni és megosztani például többszáz harmadik fél hirdető között, gyakran anélkül, hogy a felhasználó ennek tudatában lenne vagy értelmes választási lehetőséggel rendelkezne. Olyan adatokat gyüjtenek, amelyek árulkodnak a személy magánéletéről, mint például tartózkodási helyéről, vásárlási szokásairól, az általa meglátogatott honlapokról, kapcsolatairól, közösségi összeköttetéseiről.  Az Egyesült Királyság Informatikai Miniszterének Irodája (UK Information Commissioner’s Office, ICO): “A 2018 évi Európai Általános Adatvédelmi Rendelet (GDPR) **biztosítja a személyek számára a jogot, hogy tájékoztatást kapjanak személyes adataik gyűjtéséről és használatáról.** **Ez egy kulcsfontosságú átláthatósági követelmény**” – magyarázza az [ICO](https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/right-to-be-informed/) honlapja itt: <https://bit.ly/2QxmZH1>  Pat Walshe a Privacy Matters-től kijelenti: “A magánélethez és adatvédelemhez való jog ma fontosabb, mint eddig bármikor, mivel digitális adataink személyünk és kapcsolataink mélyen személyes és intim vonatkozásait árulják el.  Text, whiteboard  Description automatically generated  A kép szövege:  Az online adatvédelem ~~halott~~ az Ön emberi joga.  Mire számíthat a következő lépcsőben?  A tanfolyam utolsó lépcsőjében, az 5. lépcsőben azokról az *online eszközökről* fogunk tanulni, melyeket *adataink hatékonyabb védelmére* használhatunk.  Ellenőrizze a tanultakat!  Kérem, ellenőrizze, hogy mit tanult a 4. lépcsőben egy mini-kvíz segítségével, melyet a Feladatok részben talál! |
| Ellenőrizze tudását | **1948 Universal Declaration of Human Rights (UDHR)**: **12. paragrafus**: “Senki sem szenvedhet el önkényes beavatkozást magánéletébe (vagy) levelezésébe”.  **2000 EU Charter of Fundamental Rights (EHCR): 1. paragrafus**: “Az emberi méltóság sérthetetlen. Tisztelni és védeni kell”.  **2018 General Data Protection Regulation (GDPR)** **“magas követelményt támaszt a beleegyezéshez**”: Ez a ***tájékoztatáson alapuló*** önkéntes beleegyezés:   * “valódi választást és ellenőrzést kínál a személyek számára” * “a hiteles beleegyezésnek az egyénre kell ruháznia a felelősséget, bizalmat és elkötelezettséget kell építenie”. |
| Feladatok | **Mini-kvíz** a különböző chartákból és szabályzatokból.  A következő kijelentések igazak vagy hamisak?   * Az UNHR egy új szabályzat, mely a tájékoztatáson alapuló belegyező nyilatkozatot biztosítja. * Az ePrivacy Directive sütikre vonatkozik. * A GDPR nem foglalkozik az átláthatósággal.   Vitassa meg családjával, barátaival, szomszédaival vagy kollégáival a válaszokat.  Emlékeztető: nézeteit posztolhatja a CSI-COP honlap fórumán: <https://csi-cop.eu/forum/>. A posztoláshoz regisztrálnia kell a honlapon egy log-in létrehozásával: <https://csi-cop.eu/citizenscientistlogin/> |
| A feladatok célja | Családtagokkal, barátokkal és szomszédokkal megvitatni Scott McNealy, a Sun Microsystems vezérigazgatójának és társalapítójának 1999 évi kijelentését:  “***Amúgy is nulla magánéleted van… Lépjünk túl rajta***!”  A Wired honlapon idézve:  <https://www.wired.com/1999/01/sun-on-privacy-get-over-it/> |
| Rövid Tweet | Az online adatvédelem nem luxus. |

|  |  |
| --- | --- |
| **További olvasnivalók a 4. lépcsőhöz** | A 4. lépcsőben említett további olvasnivalók alább találhatók az aláhúzott szövegre kattintva:  **Ajánlott olvasnivalók**  British Library (2013). Taking Liberties: The struggle for Britain’s freedoms and rights. Taking Liberties – Star Items Index – Human Rights. Elérhető innen: <https://bit.ly/2QU4bSa>  ICO (no date). Guide to the General Data Protection Regulation (GDPR): Right to be informed. UK Information Commissioner’s Office (ICO). Elérhető innen: <https://bit.ly/3erd79K>  **További olvasnivalók**  EHCR (n. a.). European Convention on Human Rights. Elérhető innen: <https://www.echr.coe.int/Pages/home.aspx?p=basictexts&c=> ePrivacy Directive (2002). 32002L0058 **Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications). Elérhető angol nyelven innen:** <https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32002L0058&from=EN> GDPR (2016). REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). **Elérhető angol nyelven innen**:  <https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:02016R0679-20160504&from=EN>  UN (n. a.). United Nations Declaration of Human Rights. Elérhető innen:  [https://www.un.org/en/about-us/universal-declaration-of-human-rights]( https://www.un.org/en/about-us/universal-declaration-of-human-rights) |

### 5. lépcső

|  |  |
| --- | --- |
| 5. lépcső címe | Hogyan védjük meg adatainkat online? |
| Új ismeretek az 5. lépcsőben | 1. Az adatvédelem különböző szempontjainak leírása és megvitatása. 2. A személyes adatok gyűjtési módjának azonosítása és értékelése az interneten való szörfölés és az okos eszközök alkalmazásainak használata során. 3. Az adataink védelmét biztosító egyezményekből eredő adatvédelmi jogok megértése |
| Téma | Online eszközök adataink védelmére. |
| Fő kérdés | *Hogyan változtassam meg az app és internet beállításaimat, hogy meggátoljam az online követést?*  Kérdezze meg családját és barátait, hogy mit gondolnak az adataikról. Posztolhatja meglátásait a CSI-COP honlap fórumán: <https://csi-cop.eu/forum/>. Mielőtt posztol a fórumon, egy log-in létrehozásával regisztrálnia kell a honlapon: <https://csi-cop.eu/citizenscientistlogin/> |
| Rövid összefoglaló | **Appok**: a használt appok esetében ellenőrizze mobil eszközein a beleegyezést a ‘Beállítások’ menüpontban. Mielőtt letölt egy appot ellenőrizze, hogy milyen beleegyezéseket kér az app – szükségesek ezek az app működéséhez? Például egy közlekedési appnak hozzá kell férnie az Ön tartózkodási helyéhez, hogy pontos információt tudjon adni a közeli járatok érkezési idejéről.  Honlapok: Használjon beépített adatvédelemmel ellátott böngészőt vagy tiltsa meg a követést a beállítások frissítésével, és korlátozza a harmadik felek hirdetési és marketing sütijeit. |
|  |  |
| Tananyag | **Online eszközök, amelyek elősegíthetik adatainak és magánéletének védelmét**  Összefoglalva az előző négy lépcsőben tanultakat:   * Az 1. lépcsőben bemutattuk az ‘adatvédelem’ koncepcióját * A 2. lépcsőben megtanultuk, hogy a ‘személyes adat’ természetes (élő) személyre vonatkozik * A 3. lépcsőben azokról a módszerekről tanultunk, amelyekkel adatainkat elfogják online (pl. követést végző sütik segítségével) * A 4. lépcsőben azokról a törvényekről és rendeletekről tanultunk, melyet biztosítják az adatvédelemhez való jogot   Ebben a lépcsőben megtudjuk, hogy milyen ingyenes online eszközök állnak rendelkezésünkre adataink és magánéletünk védelmére.  Ha átgondolja saját internet használatát, érzi-e, hogy egyre inkább online folytatja életét?  Pat Walshe (Privacy Matters) megjegyzi, hogy online intézzük a következőket: vásárlás, videohívások, üzenetek küldése, élmények, gondolatok és érzések megosztása a közösségi médián keresztül. Továbbá így foglalunk időpontot orvoshoz, keresünk információt egészségi kérdéseinkre. Az online térbe megyünk akkor is, ha útirányt keresünk vagy követünk – közösségi közlekedés, autóhasználat, biciklizés vagy gyaloglás esetén. Zenét is online hallgatunk, filmeket, TV-t is az interneten nézünk.  Életünk nagy része digitális lett. De a digitálissá válás digitális lábnyomokat hoz létre és hagy, olyan digitális adatokat, amelyeket össze lehet gyűjteni és fel lehet használni profilunk elkészítésére, megismerésünkre, befolyásolásunkra oly módon, hogy nem is vagyunk tudatában. Minden honlap, amelyet meglátogat; minden kattintás és koppintás, amit végez; minden hívás vagy üzenet, melyet küld vagy fogad, minden közösségi média poszt, amelyet feltesz; a helyek, amelyeket meglátogat vagy megjelöl; minden ‘like’, amit bejelöl; a dalok, amelyeket hallgat vagy a filmek, amelyeket megnéz (és részletek arról, hogy mikor tette, szüneteltette, gyorsította fel vagy hagyta abba azokat) adatokat képez. Ezek azok az adatok, melyek megmutatják viselkedésének jellegét, az ÖN milyenségét és személyiségének intim részleteit. Például a termékenységi appok, melyek bensőségesen ismerik Önt. Lásd a Wired magazine 2018-as cikkét ‘Before using birth control apps, consider your privacy’: [https://bit.ly/3ajCyZz](https://bit.ly/3ajCyZz%20)  Egy adatvédelmi jótékonysági intézmény azt tette közzé egy 2020 évi Guardian számban, hogy ‘A menstruációs appok rendkívül sok információt tárolnak’. Itt olvashat erről:  [https://bit.ly/3aj7IQH](https://bit.ly/3aj7IQH )  Vannak olyan appok, melyek például egy személy szexualitásának, vallásosságának vagy pillanatnyi tartózkodási helyének intim vonatkozásait osztják meg (a helyszínre vonatkozó adatok nagyon sok utalást tartalmazhatnak – például a helyszín egy speciális típusú istentisztelet helye vagy egy speciális jellegű egészségügyi intézmény). Lásd a 2000 évi Fogyasztói jelentést a hasonló appokról itt: <https://bit.ly/3ggUw2x>  Vannak olyan gyermekeket és tinédzsereket/fiatal felnőtteket célzó alkalmazások is, amelyek adatokat rögzítenek, esetleg az alkalmazást letöltő gyermek vagy tinédzser tudta nélkül, illetve az adott alkalmazást a gyermekük számára megvásároló szülő(k) tudta nélkül. A Yubo egy „közösségi médiaalkalmazás”, amely gyerekeket céloz meg azzal, hogy segít nekik barátokat találni. A brit Sunday Times újság 2022. február 20-i számában számolt be az alkalmazás biztonsági problémáiról. A cikk – amelynek címe „Visszaélés a ’tinik Tinderén’” – óvja a szülőket a szociális média bizonyos applikációitól, amelyek szexuális zaklatásnak, rasszizmusnak és terrorizálásnak teszik ki a gyerekeket.  A picture containing text, newspaper  Description automatically generated  Az 5. lépcsőben később tanulunk olyan ingyenes online eszközökről, amelyek a Yubo-hoz hasonló alkalmazások mögé néznek, hogy segítsenek megállapítani, felmerülnek-e adatvédelmi problémák a gyermekeket célzó applikációk esetében.  Az adatok nemcsak ÖNre vonatkozó információkat árulnak el, hanem MÁSokra vonatkozóakat is. Azokról, akikkel kommunikál és információt oszt meg, kapcsolatairól és azoknak mintáiról. Például egy app arra kérheti, hogy töltse fel vagy adjon hozzáférést a ‘kontaktokhoz’, melyeket számítógépén vagy mobiltelefonján tárol. De mi is van ezekben? Egy ‘kontakt’ tartalmazhatja a személy nevét, fényképét, mobilszámát, e-mail címét, postai címét, közösségi média avatárját, születésnapját. Digitális online létezésünk arra kényszerít minket, hogy nemcsak a saját adataink védelmére, hanem másokéra is gondoljunk.  Ahogy a 4. lépcsőben megbeszéltük az EU-ban és az Egyesült Királyságban az online adatok védelméhez való jogot speciális **ePrivacy** törvények és az európai általános adatvédelmi rendelet (**GDPR**) biztosítja. De a törvények és végrehajtásuk csak egy bizonyos határig hatásosak. Vannak dolgok, amelyeket Ön saját maga is megtehet adatainak online védelmére.  A 3. lépcsőben tanultunk arról, hogy hogyan követik az embereket az **interneten keresztül**. Ez sokféle lehet a hirdetési technológiától, mint például a sütik, a szerver oldali követésig. De mit csinálhatunk, hogyan ellenőrizzük ezeket és védjük meg online az adatainkat? [Az [adatvédelmi önszabályozás](https://policyreview.info/pdf/policyreview-2020-4-1537.pdf) nehéz]. Többet tanulhat arról, hogy hogyan [követik](https://privacyinternational.org/case-study/4404/mobile-app-monetisation-covert-trackers-your-pocket) az embereket **mobil app**ok segítségével(software development kits - SDKs), ha elolvassa Binns és mtsai. (2018) cikkét: ‘Third Party Tracking in the Mobile Ecosystem’, mely innen érhető el: <https://arxiv.org/pdf/1804.03603.pdf> .  **Eszközök, amelyekkel a követés észlelhető vagy ellenőrizhető**  **Átláthatósági eszközök - internet:**  Számos eszköz érhető el, melyek segítenek Önnek megérteni a követést azokon a honlapokon, amelyeket meglátogat. Sok követés arra szolgál, hogy hirdetésekkel célozzák meg vagy növeljék az Ön személyre szóló élményét. Ez gyakran magában foglalja azt is, hogy adatokat osztanak meg harmadik fél hirdetőkkel, akár többszáz céggel.  **Néhány internet átláthatósági eszköz:**  A **Webbkoll** azt szimulálja, hogy mi történik, ha egy felhasználó meglátogat egy honlapot egy tipikus böngészőt használva. Megmutatja, hogy milyen elsődleges és harmadik fél sütik lehetnek jelen a meglátogatott oldalon, valamint azt is, hogy milyen, sütiktől független követés történik, amelyet például szerverek kérnek: <https://webbkoll.dataskydd.net/en>  A **Blacklight** szkenneli a honlapot, és feltárja a kulcs követési technológiákat - ezen az oldalon található: <https://themarkup.org/blacklight>  A **Pagexray** egy analitikai eszköz, mely megmutatja azokat a hirdetéseket és követőket, melyeket egy adott honlapra feltöltöttek, és az eredményt egy fa formájú grafikában jeleníti meg. Az eredményeket HTTP Archive (.har.json) formátumban vagy részletes adatokként (.json) lehet letölteni: <https://pagexray.fouanalytics.com/>  A **Request Map Generator** segít azonosítani a harmadik fél hirdetőket egy honlapon és azt, hogy hová továbbítják az adatokat. Az adatokat egy CSV fájlban lehet letölteni: <https://requestmap.webperf.tools>  A **Cover Your Tracks** olyan eszköz, amely teszteli, hogy az Ön böngészője mennyire eredményesen véd a követéssel és ujjlenyomatozással szemben: <https://coveryourtracks.eff.org>  **Átláthatósági eszközök – mobiltelefonos appok:** A mobiltelefonos appok vizsgálata nem könnyű. [O’Flaherty](https://www.forbes.com/sites/kateoflahertyuk/2021/01/31/apples-stunning-ios-14-privacy-move-a-game-changer-for-all-iphone-users/), cyber specialista újságíró szerint, ha Ön appokat használ, akkor az appok “követhetik Önt más appokon és honlapokon keresztül, azzal a céllal, hogy hirdetésekkel célozzák meg. Ezt jelenleg a hirdetők által használt azonosítóval (identifier for advertisers, **IDFA**) végzik, amely az Ön személyes adatainak felfedése nélkül végez követést”. Van néhány eszköz, mely fényt tud deríteni az Android appokba ágyazott ‘követők’ létezésére.  Az Android esetében kulcs eszköz az **Exodus Privacy**: <https://exodus-privacy.eu.org/en/>  Android stúdió: <https://developer.android.com/studio>  Pat Walshe (Privacy Matters) szerint jelenleg nincs olyan eszköz, amely ekvivalens az Apple iOS appjával. Az Apple olyan új átláthatósági szabályokat vezetett be a boltja és a fejlesztők számára, amelyek megkövetelik előre meghatározott adatvédelmi címkék használatát, melyek megmutatják, hogy milyen adatot használnak és miért. Az Apple új iOS [14.5](https://eur01.safelinks.protection.outlook.com/?url=https%3A%2F%2Fwww.apple.com%2Fnewsroom%2F2021%2F04%2Fios-14-5-offers-unlock-iphone-with-apple-watch-diverse-siri-voices-and-more%2F&data=04%7C01%7Cab7778%40coventry.ac.uk%7C0961dc6c3373461cef5308d9096cf9ba%7C4b18ab9a37654abeac7c0e0d398afd4f%7C0%7C0%7C637551185936139952%7CUnknown%7CTWFpbGZsb3d8eyJWIjoiMC4wLjAwMDAiLCJQIjoiV2luMzIiLCJBTiI6Ik1haWwiLCJXVCI6Mn0%3D%7C1000&sdata=yZzrdJ2Qdo3qBjKRGUWHNO5wjKePxo4%2BYYrWf3M4sHM%3D&reserved=0) rendszere azt is megköveteli a fejlesztőktől, hogy "*kérjék meg a felhasználó engedélyét mielőtt az adatait más cégek tulajdonában lévő, hirdetési célú appokon vagy honlapokon keresztül követik vagy azokat megosztják adat brókerekkel.*”  Az Apple szerint az új adatvédelmi funkcióval rendelkező operációs rendszerrel ellátott Apple telefonok használóinak megvan a lehetőségük, hogy “a Privacy Report gomb megnyomásával jobban megértsék, hogyan kezelik adataik védelmét a honlapok.” ([Apple, 2021](https://www.apple.com/uk/ios/ios-14/)). Ugyancsak az Apple szerint az App Tracking Transparency funkció (ATT) “minden apptól megköveteli, hogy kifejezett engedélyt kérjen a követésre” és “a felhasználók a Beállítások menüpontban látni fogják, hogy melyik app kért engedélyt a követésre, és számukra megfelelő változtatásokat eszközölhetnek.” ([O’Flaherty, 2021](https://www.forbes.com/sites/kateoflahertyuk/2021/01/31/apples-stunning-ios-14-privacy-move-a-game-changer-for-all-iphone-users/)).  Az Apple Mac operációs rendszere (‘Big Sur’) tartalmaz egy adatvédelmi jelentés funkciót, mely ikonként jelenik meg a Safari böngészőben. Ez lehetővé teszi, hogy a felhasználó lássa, milyen követők vannak a honlapon, és blokkolhatja azokat. Az Apple Safari böngészője “több lehetőséget ad az adatvédelem elősegítésére” ([Apple, 2021](https://www.apple.com/uk/ios/ios-14/)). Az Apple adatvédelmi meghajtója “gyökeres változást” hoz [O’Flaherty, 2021](https://www.forbes.com/sites/kateoflahertyuk/2021/01/31/apples-stunning-ios-14-privacy-move-a-game-changer-for-all-iphone-users/). szerint.  És a “harmadik fél süti halála” ([Cyphers, 2021](https://www.eff.org/deeplinks/2021/03/googles-floc-terrible-idea)) következtében a civil kutatók képviselhetik azt a mozgalmat, amely megelőzi az online követés bármilyen helyettesítését, mint például a Google azon “új technológiai csomagját, amely hirdetéseket céloz meg az interneten”, és ezáltal közelebb visz minket az adataink védelmével összhangban lévő böngészéshez.  **Ismétlés: Mit tehetünk adataink védelmére?**  Használjunk olyan böngészőt, amely megvédi adatainkat  Használjunk hirdetés blokkolókat  Használjunk adatvédelmi beállításokat – operációs rendszerek, böngészők, appok.  Graphical user interface, application  Description automatically generated |
| Ellenőrizze tudását | Kérem, gondolja végig, hogy mit tanult az 5. lépcsőben. Értse meg, hogy vannak különböző módszerek adatainak és magánéletének védelmére az online térben is. |
| Feladatok | Kísérletező tanulás: tanulmányozza, milyen digitális követők vannak a meglátogatott honlapokon és a használt appokon.  **1. feladat**  Használja az egyik eszközt, amelyről ebben a lépcsőben tanult, mint például a [webbkoll](https://webbkoll.dataskydd.net/)-t egy Ön által gyakran látogatott honlap hátterének felfedezésére. Vizsgálja meg a honlapot a) a használt adatvédelmi eljárás és b) a süti tájékoztatás szempontjából.  Kérdések  -Mennyire volt könnyű megérteni a használt adatvédelmi eljárást?  -Volt-e tájékoztatás a sütikről és hány sütit említettek meg? -Milyen beágyazott *harmadik fél süti* volt megemlítve a süti tájékoztatásban?  **2. feladat**  Ha Önnek van gyermeke, és engedi neki, hogy okostelefonos alkalmazásokat használjon, ellenőrizze a beleegyezéseket egy app esetében! Lehetőleg egy gyerekeknek szánt alkalmazást válasszon, pl. valamilyen játékos, vagy barátkozós applikációt! Menjen a ‘Beállítások’-hoz és válassza ki bármelyik appot, majd ellenőrizze a beleegyezéseket!  Kérdések  -Milyen beleegyezéseket kért a megvizsgált app?  -Tisztában volt ezekkel a beleegyezésekkel, amikor az appot letöltötte?  Emlékeztető: nézeteit posztolhatja a CSI-COP honlap fórumán: <https://csi-cop.eu/forum/>. A posztoláshoz regisztrálnia kell a honlapon egy log-in létrehozásával: <https://csi-cop.eu/citizenscientistlogin/> |
| A feladatok célja | Informális tanulóból CSI-COP civil kutatóvá válni.  Beszélje meg családjával és barátaival a tanfolyammal kapcsolatos véleményét:   * Hogyan érzi, mit sajátított el a CSI-COP öt, informális oktatási lépcsőjében? * Szeretne-e a CSI-COP csapathoz csatlakozni és civil kutatóként az online követést vizsgálni? * Érdekelné-e további oktatás az adatvédelemmel, weblap- és alkalmazás fejlesztéssel és hasonló témákkal kapcsolatban? |
| Rövid Tweet | Internetes alapú eszközökkel védem adataimat. |
| **További olvasnivalók a 5. lépcsőhöz** | **Ajánlott olvasnivalók**  Cyphers, B. (2021). Google’s FLoC (Federated Learning of Cohorts) is a terrible idea. **Electronic Frontier Foundation**. Letölthető innen: <https://www.eff.org/deeplinks/2021/03/googles-floc-terrible-idea>  O’Flaherty, K. (2021). Apple’s Stunning iOS14 Privacy Move: a game-changer for all iPhone Users. **Forbes**. Letölthető innen: <https://bit.ly/3vpOq4v/> |

Visszajelzés

|  |  |
| --- | --- |
| Az Ön visszajelzése a CSI-COP „Az online adatvédelemhez való jog” című, informális oktatást nyújtó tanfolyamáról | Nagyban segítené a CSI-COP csapatot, ha megosztaná velünk, mennyire találta hasznosnak a tanfolyamot. Kérjük, jelöljön be egy választ az alábbiak közül:  5. Nagyon hasznos  4. Hasznos  3. Nincs véleményem  2. Nem hasznos  1. Egyáltalán nem hasznos  Kérjük, bátran írja le a tanfolyammal kapcsolatos egyéb megjegyzéseit vagy javaslatait: |

### Ellenőrző kérdések

A tanultak ellenőrzéséhez és a CSI-COP bizonyítvány megszerzéséhez kérjük, válaszoljon az alábbi kérdésekre.

A kérdések letölthető word formátumban külön is elérhetőek.

A CSI-COP informális oktatást nyújtó tanfolyamának elvégzéséről szóló bizonyítvány megszerzésének feltétele:

* **10-ből** legalább **8 kérdésre** **helyesen kell válaszolni,**
* **a válaszokat az alábbi email címre szükséges továbbítani**:

Máriának: [mhinsenkamp71@gmail.com](mailto:mhinsenkamp71@gmail.com) vagy

Dorkának: dorottya\_rigler@yahoo.com.

A kérdések megválaszolásával tetszőleges alkalommal próbálkozhat.

**Kérdések**

* 1. Igaz vagy hamis a következő állítás? Az adatvédelem a Facebook megjelenése óta vált problémává.

IGAZ / TRUE HAMIS / FALSE

* 1. Igaz vagy hamis a következő állítás? A Google Chrome Incognito böngészője lehetővé teszi, hogy Ön teljeskörű adatvédelem mellett kereshessen.

IGAZ / TRUE HAMIS / FALSE

* 1. Igaz vagy hamis a következő állítás? A nyilvános wi-fi megoszthatja az Ön helyadatait.

IGAZ / TRUE HAMIS / FALSE

* 1. Igaz vagy hamis a következő állítás? Az érzékeny személyes adatok az Ön nevéhez kapcsolódnak.

IGAZ / TRUE HAMIS / FALSE

* 1. Igaz vagy hamis a következő állítás? Az ujjlenyomat a weboldalakon végzett nyomkövetés egy formája, amely az Ön eszközének vagy böngészőjének attribútumai alapján profilt készít Önről.

IGAZ / TRUE HAMIS / FALSE

* 1. Mi minősül viselkedési adatnak? Kérjük, válassza ki az alábbi listáról az összes idetartozó elemet!
     1. Az Ön interakciói egy weboldalon
     2. Az Ön internetes böngészési adatai
     3. Online vásárlási előzmények
     4. Online térkép használata
     5. Alkalmazás használata, pl. az egészsége monitorozása céljából.
  2. Igaz vagy hamis a következő állítás? Az emberi jogokat nélkülözhetetlennek tekintették méltóságunk szempontjából, illetve az alapvető szabadságjogok védelméhez.

IGAZ / TRUE HAMIS / FALSE

* 1. Igaz vagy hamis a következő állítás? Az Emberi Jogok Egyetemes Nyilatkozata (Universal Declaration of Human Rights - UDHR) magában foglalja a következőkhöz való jogot: „védelem az egyének magánéletébe, családjába, otthonába vagy levelezésébe való önkényes beavatkozás ellen”.

IGAZ / TRUE HAMIS / FALSE

* 1. Igaz vagy hamis a következő állítás? Az emberi jogok európai egyezménye (European Convention on Human Rights – ECHR) értelmében a modern korban nincs jogunk elvárni, hogy otthonunkban és levelezésünkben magán- illetve családi életet élhessünk.

IGAZ / TRUE HAMIS / FALSE

* 1. Kérjük, válassza ki az összes olyan elemet, amelyre az általános adatvédelmi rendelet (General Data Protection Regulation - GDPR) kiterjed:
     1. Tájékoztatáshoz való jog
     2. Átláthatósághoz való jog
     3. Adatvédelemhez való jog
     4. Ahhoz való jog, hogy mások eszközeivel ne készüljön rólunk filmfelvétel.

Hogyan lehet civil kutatóvá válni?

|  |  |
| --- | --- |
| **Hogyan lehet civil kutatóvá válni?** | A CSI-COP öt lépcsős, informális oktatást nyújtó tanfolyamának elvégzése és a bizonyítvány kézhezvétele után szeretettel várjuk, ha csatlakozna a CSI-COP csapathoz, és segítene nekünk az online nyomkövetés mértékének vizsgálatában.  Lehetősége van csatlakozni a CSI-COP csapathoz, és önkéntes civil kutatóként szerepet vállalni a CSI-COP projektben.  Kérésére teljeskörű tájékoztatást nyújtunk Önnek az alábbiakban:   * Tájékoztató levél az önkéntes résztvevők számára a civil kutatók szerepéről * Az általános adatvédelmi rendeletnek (General Data Protection Regulation – GDPR) megfelelő, tájékoztatáson alapuló beleegyező nyilatkozat * Tájékoztatás arról, hogyan érdemes elkezdeni a sütik vizsgálatát a weboldalakon és az alkalmazásokban.   További információkat talál a CSI-COP weboldalának ['About'](https://csi-cop.eu/about/) menüpontjában: <https://csi-cop.eu/about/>. Ajánljuk a Gyakran Ismételt Kérdések (GyIK) elolvasását is a weboldalon: <https://csi-cop.eu/faq/>  Ha még nem jelezte érdeklődését, az alábbi linken regisztrálhat a CSI-COP weboldalán egy felhasználói fiók létrehozásával: <https://csi-cop.eu/citizenscientistlogin/>.  Az alábbi linken érhető el a CSI-COP fóruma, ahol a többi civil kutatóval beszélgethet:  <https://csi-cop.eu/forum/>.  Nagyon köszönjük, hogy idáig velünk tartott. Van még egy feladatunk, amiben szeretnénk segítségét kérni: megtudni, kik jelentkeznek civil kutatónak. A következő oldalakon egy kérdőívet talál. Felhívjuk figyelmét, hogy nem teszünk fel olyan kérdéseket, amelyek alapján Ön azonosítható lenne. Nagyra értékeljük, ha időt szán arra, hogy a kérdőív kitöltésével segítse munkánkat. Örömmel várjuk, hogy civil kutatóként és jövőbeli adatvédelmi bajnokként csatlakozzon a CSI-COP-hoz.  Mária, Dorka, Huma és Jaimz |

**CSI-COP 1. kérdőív**

|  |  |
| --- | --- |
| **Korcsoport: kérjük, karikázza be a megfelelő korcsoportot!**  **Age range: please circle one from the range** | 18-39; 40-65; 66+; Nem válaszolok  18-39; 40-65; 66+; Prefer not to say |
| **Nem: kérjük, válasszon egyet!**  **Gender: please select one** | Nő; Férfi; Interszexuális; Transznemű; Egyéb; Nem válaszolok  Female; Male; Intersex; Trans Umbrella; Other; Prefer not to say |
| **Lakóhely: kérjük, válasszon egyet!**  **Location: please select one** | Város – kis- vagy nagyváros, pl. Patras, Coventry, London  Vidék – 2000 fő alatti kistelepülés  Nem válaszolok  Urban – towns and cities -e.g. Patras, Coventry, London  Rural – villages (below 2000 population)  Prefer not to say |
| **Nyelvek:**  **1.** Mi az elsődlegesen használt, illetve anyanyelve?  **2.** Milyen más nyelve(ke)n beszél folyékonyan?  Nem kötelező válaszolnia.  **Languages:**   1. What is your dominant, or mother tongue? 2. Do you speak more than one language fluently?   **You can prefer not to say.** | **1.**  **2.**  Nem válaszolok.  **1.**  **2.**  Prefer not to say |
| **Akadályozottság:**  Küzd-e valamilyen típusú akadályozottsággal, pl. használ-e írott szöveget beszéddé alakító programot látási nehézségek miatt?  **Accessibility:**  Do you regard yourself as having some accessibility issues; for example, use text-to-speech software due to a visual impairment? | IGEN  NEM  Nem válaszolok  YES  NO  Prefer not to say |
| **Munka:**  **Work:** | Diák: kérjük, válasszon az alábbiak közül:  Alapképzés  Posztgraduális képzés  Doktori képzés  Nem diák: kérjük, válassza ki az alábbiak közül a munkaerőpiaci státuszának leginkább megfelelő kategóriát:  Foglalkoztatott, legalább heti 36,5 órában  Foglalkoztatott, heti 1-36 órában  Nem foglalkoztatott, munkát keres  Nem foglalkoztatott, nem keres munkát  Menedékjogra vár  Nyugdíjas  Fogyatékossággal élő, munkaképtelen  Nem válaszolok  Student level: please select  Undergraduate  Postgraduate  Doctoral  Non-student: please select the category that best describes your employment status:  Employed, working 36.5 or more hours per week  Employed, working 1-36 hours per week  Not employed, looking for work  Not employed, not looking for work  Refugee seeking asylum  Retired  Having accessibility issues, not able to work  Prefer not to say |
| **Internet elérés:**  **Internet access:** | Saját internet eléréssel rendelkezem (otthoni vagy munkahelyi szélessáv/mobil internet)  Közösségi internetfelhasználó vagyok  Nem válaszolok  Have access to own Internet connection (home or work broadband/mobile)  Use public access when using the Internet  Prefer not to say |
| **Internet használat:**  Milyen gyakran használja az internetet? Kérjük, válasszon!  **Internet usage:**  How often do you use the Internet? Please select: | Naponta  Hetente 2-3 alkalommal  Hetente egyszer  Hetente egy alkalomnál ritkábban  Soha  Nem válaszolok  Daily  2-3 times a week  Once a week  Less than once a week  Never  Prefer not to say |
| **Az internet használat célja:**  **Purpose of Internet use:** | A napi munka részeként használom az internetet  Szabadidőmben használom az internetet, a munkámhoz nincs szükség rá  Munkához és szabadidős tevékenységként használom az internetet  Korlátozottan használom az internetet, pl. könyvtárban  Nem válaszolok  Use the Internet as part of daily work  Use the Internet for leisure, not part of work  Use the Internet for work and leisure  Use the Internet in a limited way, for example, using a computer in a public library.  Prefer not to say |
| **Alkalmazások használata asztali számítógépen és laptopon**  **Apps usage: Desktops and laptops** | Rendszeresen használok alkalmazásokat, például munkaeszközökhöz való hozzáférés hitelesítéséhez (pl. Zoom, Ms Teams). - Kérjük, adja meg néhány Ön által használt alkalmazás nevét és célját:  Munkaeszközök (pl. Microsoft Office  stb.)  Játékok (pl. STEAM)  Oktató alkalmazások  Életmód (sport, fitnesz, egészség)  Hírek  Szórakozás (pl. streaming alkalmazások, ld. Netflix)  Egyéb  Nem válaszolok  Ritkán használok alkalmazásokat asztali számítógépen vagy laptopon  Nem használok alkalmazásokat asztali számítógépen vagy laptopon  Nem válaszolok  Use apps regularly, for example to authenticate access to work tools (e.g. Zoom, MS Teams). If so please provide names of some apps you use and their purpose:  Work tools (e.g. Microsoft Office, etc.)  Playing Games (e.g. STEAM).  Educational apps  Lifestyle (sport, fitness, health)  News  Entertainment (e.g. streaming apps, such as Netflix)  Other  Prefer not to say  Rarely use apps on desktops and laptops  Do not use apps on desktops and laptops  Prefer not to say |
| **Alkalmazások használata mobilkészülékeken**  **Apps usage: Mobile devices** | Rendszeresen használok alkalmazásokat, pl. közlekedési applikációkat, hogy megnézzem a következő busz/vonat/stb. indulásának időpontját. - Kérjük, adja meg néhány Ön által használt alkalmazás nevét és célját:  Játékok  Oktató alkalmazások  Életmód (sport, fitnesz, egészség)  Hírek  Szórakozás (pl. streaming alkalmazások – Amazon Prime)  Egyéb  Nem válaszolok  Ritkán használok alkalmazásokat mobiltelefonon vagy táblagépen  Nem használok alkalmazásokat  Nem válaszolok  Use apps regularly, for example, transport apps to inform on timing of next train, bus, etc. If so please provide names of some apps you use and their purpose:  Playing Games  Educational apps  Lifestyle (sport, fitness, health):  News  Entertainment (e.g. streaming apps – Amazon Prime):  Other  Prefer not to say  Rarely use apps on mobile phone or tablet  Do not use apps  Prefer not to say |
| **Hol hallott a CSI-COP projektről?**  **How did you hear about the CSI-COP project?** | A CSI-COP weboldalán  Egyetemen  Egy egyesületben (pl. Women in Tech)  Egy civil kutatási platformon, például:   * SciStarter * Zooniverse * EU-Citizen.Science * Egyéb civil kutatási platform   Az interneten szörfözve  Korábbi önkéntes munka során  A közöségi médiában – kérjük, nevezze meg, melyik platformon!  Meséltek róla  Egyéb  From CSI-COP website  From a university  From membership to an association (e.g. Women in tech)  From a citizen science platform, for example   * SciStarter * Zooniverse * EU-Citizen.Science * Other citizen science platform   Surfing the web  Previous voluntary work  From Social media, please say which platform  Word-of-mouth  Other |
| **Elvégezte a CSI-COP ingyenes, online, informális oktatást nyújtó tanfolyamát?**  **Did you complete CSI-COP’s free online informal education workshop?** | Igen  Még nem, de szeretném  Nem, inkább jelenléti workshopon szeretnék részt venni, ha a lakóhelyemhez közel tartják  Yes  Not yet but intend to  No, prefer to wait for future face-to-face workshops if held near to where I live |
| **Amennyiben már elvégezte a workshopot, szándékában áll csatlakozni a CSI-COP csapatához önkéntes civil kutatóként?**  **If you did complete the workshop, do you intend to join the CSI-COP team as a volunteer citizen scientist?** | Igen  Talán  Több információra van szükségem  Nem  Yes  Maybe  I need more information  No |
| **Az „Ellenőrző kérdések”, valamint a kitöltött kérdőív visszaküldéséhez kérjük vegye fel a kapcsolatot a Coventry Egyetem CSI-COP csapatával. Bármely egyéb kérdéssel kérjük, forduljon a NaTE CSI-COP csapatához.** | Kérjük, küldje vissza ezt a dokumentumot kitöltve a  NaTE CSI-COP csapatnak az alábbi címek valamelyikére:  Maria: [mhinsenkamp71@gmail.com](mailto:mhinsenkamp71@gmail.com), vagy Dorka: [dorottya\_rigler@yahoo.com](mailto:dorottya_rigler@yahoo.com). |
| **Köszönjük a CSI-COP informális oktatást nyújtó tanfolyamának elvégzésére és a kérdőív kitöltésére szánt idejét!**  **Ez a dokumentum hamarosan más nyelveken is elérhetővé válik.**  **Kérjük, keresse fel a CSI-COP weboldalt:** [**https://csi-cop.eu/**](https://csi-cop.eu/) | |